Kalle Helin

Microsoft Forefront Endpoint Protection 2010

-tietoturvaratkaisun käyttöönotto

Metropolia Ammattikorkeakoulu
AMK-insinööri
Tietotekniikka
Insinöörityö
28.11.2011

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Kalle Helin Microsoft Forefront Endpoint Protection 2010 -tietoturvaratkaisun käyttöönotto 53 sivua + 1 liite 28.11.2011
Tutkinto	AMK-insinööri
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoliikennetekniikka
Ohjaaja(t)	Yliopettaja Antti Koivumäki IT-päällikkö Pekka Karppinen

Tämän insinöörityön tarkoituksena oli Microsoftin Forefront Endpoint Protection 2010:n käyttöönotto opetusympäristössä. Työ tehtiin Helsingin palvelualojen oppilaitokselle. Työn tavoite oli saada Forefront Endpoint Protection 2010:n tarjoama keskitetty tietoturvaratkaisu toimimaan koulun palvelinympäristössä.

Työn teoriaosuus käsittelee yleisiä tietoturvauhkia sekä niiden torjuntaa. Teoriassa myös käydään läpi muun muassa ohjelmistoja, joita tarvitaan asennustyössä, jotta lukijalle olisi selvempää seurata työnkulkua. Työssä käytettiin ainoastaan internet-lähteitä.

Suurin osio insinöörityöstä liittyy Forefront Endpoint Protection 2010:n asennukseen ja käyttöönottamiseen. Molemmat osiot käydään läpi kattavasti kuvien kera, jotta työn seuraaminen olisi mahdollisimman ymmärrettävää. Lopuksi vielä testataan järjestelmän toimivuutta ja verrataan sen nopeutta käytössä olevaan F-Securen järjestelmään.

Forefront Endpoint Protection 2010 saatiin onnistuneesti asennettua koulunverkkoon, mutta palvelinpäivityksien vuoksi Helsingin palvelualojen oppilaitos aikoo ottaa sen käyttöön vasta myöhemmin. Tällöin tullaan käyttämään 2012 versiota, mutta tässä työssä olevat ohjeet pätevät uuteen versioon suurimmilta osin.

Avainsanat	Microsoft, Forefront, Tietoturva, FEP, SCCM, Reporting Services

Metropolia

Abstract

Author(s) Title Number of Pages Date	Kalle Helin Microsoft Forefront Endpoint Protection 2010 53 pages + 1 appendix 28 November 2011
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunications
Instructor(s)	Antti Koivumäki, Principal Lecturer Pekka Karppinen, IT Chief

The meaning of this project was to deploy Microsoft Forefront Endpoint Protection 2010 in a school environment. The project was carried out for Helsingin palvelualojen oppilaitos. The aim of the project was to integrate the Forefront Endpoint protection 2010 centralised data security solution into the current server infrastructure.

The theoretical part of the project covers common data security threats and how to defend against them. The theory also explains the software needed in the installation work so the reader could follow the work easier. Only Internet sources were used for the project.

The biggest part of the text deals with the installation and deployment of Forefront Endpoint Protection 2010. Both topics are covered with pictures and details to facilitate the understanding of the process. Eventually Forefront Endpoint Protection 2010 is a test against F-Secure data security system which is in use already. The two products are compared in detail for speed and effectiveness.

Forefront Endpoint Protection 2010 was successfully installed and deployed on the school's network but due to upcoming server updates it will not be implemented until later in 2012. The 2012 version's installation and deployment process should be quite similar with the 2010 version so the methods discussed in this project should be applicable with it.

Keywords	Microsoft, Forefront, Tietoturva, FEP, SCCM, Reporting Services

Sisällys

Lyhenteet

b	bitti, pienin mahdollinen informaation yksikkö. Bitillä on kaksi mahdollista arvoa, joita kuvaavat yleensä ykkönen ja nolla.
B	tavu, kahdeksan bitin muodostama informaation yksikkö.
FEP	Forefront Endpoint Protection. Microsoftin tietoturvaohjelmisto.
Flash	Adoben luoma web-pohjainen multimediaohjelmointialusta. Käytetään yleisesti verkossa julkaistuun graafiseen materiaaliin.
Java	Sun Microsystemsin luoma olio-ohjelmointikieli.
SCCM	System Center Configuration Manager. Microsoftin keskitetty hallintaohjelmisto suurien laitemäärien ylläpitämiseen.
SQL	Structured Query Language. Ohjelmointikieli tietokantojen hallintaa varten.
URL	Uniform Resource Locator. Internetissä olevan sivuston tai tiedoston sekä näiden käyttöön tarvittavan yhteiskäytännön yksilöivä tunnus. WWW-sivun osoite.
WQL	Windows Management Instrumentation Query Language on johdannaiskieli SQL-kielestä.

1 Johdanto

Nykyaikana yrityksiä ja yksityiskäyttäjiä uhkaa jatkuva haittaohjelmien, hakkerien ja virusten tulva internetistä. Ilman palomuuria, virustentorjuntaa ja käyttäjienhallintaa nykyajan tietoverkot eivät pysyisi kauaa pystyssä. Missä yksityiskäyttäjät pystyvät hoitamaan tietoturvan kuntoon helposti asentamalla esimerkiksi F-Secure-virustorjuntaohjelmiston, niin yrityksillä ja laitoksilla asiat eivät ole niin yksinkertaisia. Yleensä on kyse sadoista tietokoneista, jotka täytyisi turvata ja päivittää keskitetysti, koska muuten ongelmatilanteissa vian löytäminen ja yleinen ylläpito olisi liian työlästä.

Keskitetty hallinta on ainoa järkevä ratkaisu, jos turvattavia tietokoneita on satoja. Microsoft Forefront tarjoaa tähän tarkoitukseen alan kehittyneimmän ja helpoiten hallittavan ratkaisun. Se myös integroituu ongelmitta jo olemassa olevien tietoturvaratkaisujen kanssa. Tuotteen asennus ja käyttöönotto on suoraviivaisempaa kuin muiden ratkaisujen, koska muun muassa hallinta on integroitu yhteen Microsoft Configuration Managerin kanssa.

Tämä opinnäytetyö käsittelee Microsoft Forefront -tietoturvaohjelmiston käyttöönottoa Helsingin palvelualojen oppilaitoksen verkossa ja turvattavia tietokoneita on noin pari sataa. Opinnäytetyö perehdyttää Microsoft Forefront -tietoturvaratkaisun tarvittavien ohjelmistojen asentamiseen, testaamiseen ja lopulta käyttöönottoon. Projektin pääasiallinen tarkoitus on korvata nykyään käytössä oleva F-Securen keskitetty tietoturvaratkaisu, koska Microsoft Forefront tarjoaa enemmän ja on keskitetymmin hallittavissa.

Helsingin palvelualojen oppilaitos, Helpa, on suomen suurin ammattikoulutusta tarjoava oppilaitos. Sen tarjontaan kuuluvat ravintola- ja cateringala, elintarvikeala, vaatetusala ja kauneudenhoitoala. Opiskelijoita on noin 1800, opettajia 140 ja muuta henkilökuntaa 30.

Tässä työssä oletetaan, että lukijalla on perustason ymmärrys palvelinarkkitehtuureista ja toiminnoista. Työssä ei ole tarkoitus perehtyä esimerkiksi SQL-palvelimen toimintaan tai Microsoft Configuration Managerin käyttämiseen kuin niiltä osilta, jotka ovat tarpeellisia työnkululle.

2 Tietoturvauhat

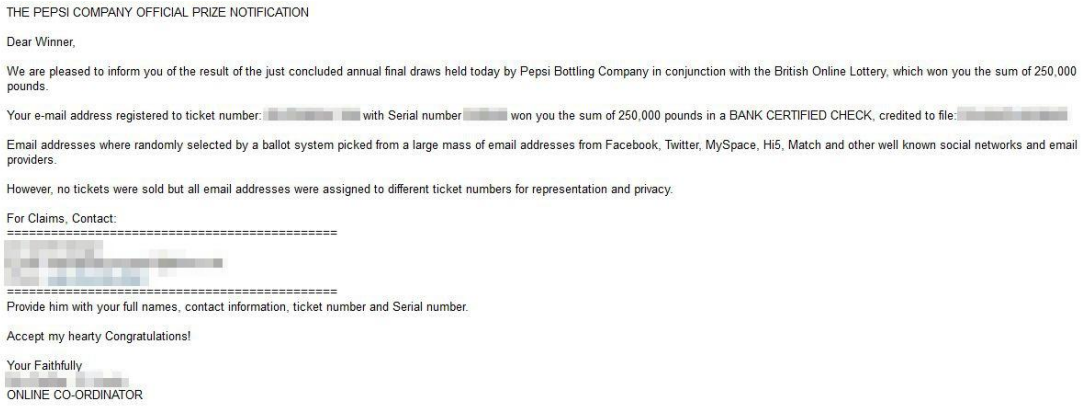
Tämän luvun tarkoituksena on pohjustaa lukija eri tietoturvauhille. Luvussa myös käydään läpi, millä perustoimenpiteillä uhkia voi välttää tai ehkäistä. Lukijan pitäisi saada peruskäsitys eri uhkatilanteista.

2.1 Uhkien perusteet

Oli kyseessä kotona oleva perheen tietokone tai yrityksen palvelin, molempia yhdistää samat vaarat internetistä. Kun tietokone yhdistetään verkkoon, se on saman tien näkyvillä mahdollisille haittaohjelmille tai hakkereille. Tämän vuoksi virustorjuntaohjelmisto ja palomuuri ovat vaadittavat minimivaatimukset mille tahansa tietokoneelle, joka on yhteydessä verkkoon.

Ensisijaisen tärkeää on myös käyttöjärjestelmän ja ohjelmistojen päivittäminen säännöllisesti. Hakkerit ja haittaohjelmat usein hyödyntävät esimerkiksi vanhentuneen selainversion tietoturva-aukkoja ja pääsevät näin aiheuttamaan tuhoja tietokoneelle. Vaikka ohjelmistot toimisivat normaalisti ilman päivityksiä, se ei tarkoita, että ne olisivat turvassa verkkouhilta. Varsinkin selaimen käyttämät Java- ja Flash-versiot on syytä päivittää ajan tasalle aina kuin mahdollista, koska molemmat ovat usein käytössä verkon haittaohjelmien levittämiseen.

Verkossa on myös sosiaalisia hakkereita. Sosiaalinen hakkerointi tarkoittaa käyttäjää, joka yrittää psykologisin keinoin päästä käsiksi uhrin käyttäjätunnuksiin, salasanoihin tai muihin yksityistietoihin. Sosiaalisia hakkereita on varsinkin yhteisösivustoilla ja pikaviestimissä, joista parhaat esimerkit ovat Facebook ja Microsoft MSN. Huijarit usein yrittävät saada uhrin tiedot käsiin lähettämällä linkin, joka johtaa haittaohjelmaan tai niin sanotulle phising-sivustolle. Kyseiset linkit on yleensä muotoiltu näyttämään harmittomilta ja niissä viitataan esimerkiksi ystävään tai sukulaiseen. Aiheena voi myös olla olemattoman palkinnon lunastaminen ja sitä kautta tietojen kalastelu (kuvio 1). (1.)



THE PEPSI COMPANY OFFICIAL PRIZE NOTIFICATION

Dear Winner,

We are pleased to inform you of the result of the just concluded annual final draws held today by Pepsi Bottling Company in conjunction with the British Online Lottery, which won you the sum of 250,000 pounds.

Your e-mail address registered to ticket number: with Serial number won you the sum of 250,000 pounds in a BANK CERTIFIED CHECK, credited to file:

Email addresses where randomly selected by a ballot system picked from a large mass of email addresses from Facebook, Twitter, MySpace, Hi5, Match and other well known social networks and email providers.

However, no tickets were sold but all email addresses were assigned to different ticket numbers for representation and privacy.

For Claims, Contact:
==========

==========
Provide him with your full names, contact information, ticket number and Serial number.

Accept my hearty Congratulations!

Your Faithfully
ONLINE CO-ORDINATOR

Kuva 1. Kuvassa esimerkkinä huijaussähköpostiviesti, jossa mainitaan rahapalkinnon voittamisesta Pepsin järjestämässä lotossa. Tarkoituksena on saada uhri lähettämään tiedot huijarille mahdollista identiteettivarkautta, tai vastaavaa varten.

Phishing-termi viittaa verkkourkintaan yleensä valesivuston kautta, joka näyttää samalta kuin kohdesivusto. Esimerkiksi pankit joutuvat usein verkkourkinnan kohteiksi, jolloin asiakkaille lähetetään sähköpostiin viesti, jossa vaaditaan heitä kirjautumaan sisälle palveluun yleensä jonkin tekaistun verukkeen perusteella. Viesti sisältää linkin väärälle sivulle, jolloin sinne syötetyt pankkitiedot tallentuvat rikollisen palvelimelle. Urkintaviestin voi yleensä tunnistaa huonosta kieliasusta tai tarkistamalla lähettäjän sähköpostiosoite. Myöskään pankit tai muut vastaavat toimijat eivät koskaan lähetä sähköpostiviestejä, joissa vaadittaisiin käyttäjätietoja. Virallisissa sähköpostiviesteissä asiakkaan nimi aina mainitaan, mutta huijausviesteissä uhria usein kutsutaan ystävänä tai asiakkaana ilman nimeä. (2.)

2.2 Salasanat ja brute-force-hyökkäykset

Viimeisenä muttei vähimpänä on erittäin tärkeää käyttää vahvoja salasanoja. Salasanan tulisi olla vähintään 8-merkkinen, joka sisältää isoja sekä pieniä kirjaimia ja numeroita. Lisäturvana voi myös käyttää erikoismerkkejä, jos palvelu niitä tukee. Sanakirjasanoja tulisi välttää eniten, koska hakkeri pystyy murtamaan heikot salasanat silmän räpäyksessä. Samaa salasanaa ei myöskään tulisi käyttää eri palveluissa.

Hakkerit käyttävät niin sanottuja sanakirja- ja brute-force-hyökkäyksiä salasanojen avaamisen. Sanakirjahyökkäyksessä ohjelma tarkistaa, onko kohteen salasana jokin sanakirjan sana. Esimerkkejä ovat muun muassa nimet, esineet, eläimet ja niin edelleen. Ohjelma myös tarkistaa usein käytettyjä variaatioita sanoista. Esimerkiksi o-kirjain on muutettu nollaksi.

Brute-force-hyökkäyksessä ohjelma permutoi kaikki mahdolliset vaihtoehdot merkki-merkiltä. Tämän takia salasanan pituudella on suuri merkitys. Mitä pidempi salasana, sitä kauemmin täytyy iteroida. Salattujen tiedostojen tulisi olla vähintään 128-bittisiä, jotta ne olisivat turvassa brute-force-hyökkäykseltä (taulukko 1).

Taulukko 1. Symmetrisen avaimen pituus brute-force-hyökkäystä vastaan.

Avaimen koko bitteinä	**Permutaatiot**	**Salauksen purkunopeus laitteelle, joka suorittaa 2^{56} permutaatiota sekunnissa.**
8	2^8	0 millisekuntia
40	2^{40}	0,015 millisekuntia
56	2^{56}	1 sekunti
64	2^{64}	4 minuuttia ja 16 sekuntia
128	2^{128}	149 745 258 842 898 vuotta
256	2^{256}	$(50\ 955\ 671\ 114\ 250\ 100)^{36}$ vuotta

Taulukosta voi nähdä, että 128-bittinen avain on nykyaikana brute-force-hyökkäyksiä vastaan turvallinen. Tosin teknologian kehittyessä laitteiden laskentateho nousee, joka mahdollistaa entistä monimutkaisimpien salauksien murtamisen. (3.)

3 Tarvittavia esitietoja

Tässä luvussa käsitellään mahdollisia aiheita ja käsitteitä, joita tarvitaan työn aikana. Ensiksi tutustutaan Microsoft Forefront Endpoint protection 2010 -ohjelmistoon ja tämän jälkeen on katsaus siihen, mikä merkitys on Microsoft Configuration Managerilla ja

Reporting Services -palvelulla projektin kannalta. Tarkoituksena on antaa selkeämpi yleiskuva työnkululle.

3.1 Forefront Endpoint Protection

Forefront Endpoint Protection 2010 on ohjelmisto, jonka tarkoituksena on suojata käyttäjät ja palvelimet keskitetysti haittaohjelmia ja verkkohyökkäyksiä vastaan. FEP 2010 on integroitu täysin hallittavaksi Microsoft System Center Configuration Manager 2007:n kautta. FEP 2010 tarjoaa erinomaiset hallintatyökalut tietoturvan ylläpitämiseen ja verkon tarkkailuun. (4.)

Koska FEP 2010 on hallittavissa yhdeltä palvelimelta, se vähentää verkonrakenteen monimutkaisuutta ja yksinkertaistaa tietoturvan hallitsemista huomattavasti. Esimerkiksi F-Securen vastaava tietoturvaratkaisu vaatii oman hallintapalvelimen muiden rinnalle. Hallinnan helppous ja palvelun integrointi ovat ensisijaisia syitä, miksi FEP 2010 voisi olla parempi vaihtoehto F-Securen tai muiden vastaavien keskitettyjen tietoturvapalvelujen tilalle Microsoft Windows -palvelinympäristössä.

Forefront-tuoteperheeseen kuuluu myös muita tietoturvaan liittyviä ohjelmistoja. Näistä kaikki integroituvat SCCM-palvelimelle kuten FEP 2010. Tässä projektissa olikin aluksi ideana asentaa myös Forefront Identity Manager käyttäjienhallintaa varten, sekä Forefront Endpoint Protection 2010 for Exchange Server sähköpostin suojaamiseen. Lopulta päädyttiin vain FEP 2010:n asentamiseen, koska muutoin projektista olisi tullut liian laaja.

3.2 Microsoft Configuration Manager

System Center Configuration Manager on Microsoftin keskitetty työasemien hallintaohjelmisto. Sen avulla on mahdollista hallita suuria määriä Windows-laitteita tietoverkossa. Configuration Managerilla on muun muassa ohjelmien etäasentaminen ja tietoverkon infrastruktuurin hallitseminen vaivatonta. Hallinnan piiriin kuuluvat tavalliset pöytäkoneet, mobiililaitteet ja virtuaaliratkaisut. Tietoverkon hallintakustannukset voivat laskea huomattavasti, jos käytössä on keskitetty hallintatyökalu vikojen havaitsemiseen tai ohjelmistojen levittämiseen. (5.)

Projektissa oli välttämätöntä opetella Configuration Managerin luonteva käyttö. FEP 2010:n hallintapaneelin käytön lisäksi täytyi käyttää ohjelmiston muita ominaisuuksia. Näihin kuuluivat tarvittavien palvelinroolien lisääminen, kokoelmien ja raporttien luominen sekä ohjelmien mainostaminen.

3.3 Reporting Services

Reporting Services on Microsoft SQL-palvelimille tarkoitettu ominaisuus, joka mahdollistaa raporttien helpon luomisen saatavilla olevista tiedoista esimerkiksi printtaustarkoitukseen. Reporting Services -palvelua hallitaan web-pohjaisella etäohjelmalla, jossa uusia raportteja voidaan luoda tai olemassa olevia hallita. Reporting Services tarjoaa myös kattavat raportointityökalut SCCM-palvelimelle. (6.)

FEP 2010 käyttää Reporting Services -ominaisuutta tietojen raportoimiseen. Tämä mahdollistaa kattavien listauksien ja raporttien luomisen esimerkiksi saastuneiden tietokoneiden tiedoista. Reporting Services -ominaisuuden asentaminen tullaan käsittelemään seruaavassa luvussa.

4 Asennus

Tässä luvussa käydään läpi Microsoft Forefront Endpoint Protection 2010:n asennustoimenpiteet. Siinä selvitetään muun muassa tarvittavat laitteistovaatimukset, ohjelmistoversiot, päivitykset ja konfiguraatiot. Asennuksen yhteydessä olevat mahdolliset ongelmatilanteet käydään myös lävitse.

4.1 Laitteistovaatimukset

Ensimmäinen toimenpide kaikissa tietotekniikan asennustehtävissä on tarkistaa vaadittavat laitteistovaatimukset. Jos kokoonpano ei ole vaatimuksien mukainen, niin asennuksen epäonnistuminen on hyvin mahdollista. Pahimmillaan siitä voi seurata laitteiston rikkoutuminen.

Microsoft Forefront Endpoint Protection 2010 asennetaan jo olemassa olevaan palvelininfrastruktuuriin. Tarvittavat palvelimet käyttöönottoa varten ovat SCCM -palvelin tiedonhallintaan ja SQL-palvelin tiedontallentamiseen ja -ylläpitämiseen. Seuraavassa taulukossa esitetään Forefront Endpoint Protection 2010 palvelin/client peruslaitteistovaatimukset (taulukko 2). (7.)

Taulukko 2. Forefront Endpoint Protection 2010 laitteistovaatimukset. Lisätietoa löytyy osoitteesta http://technet.microsoft.com/en-us/library/ff823876.aspx.

FEP10 laitteistovaatimukset	
Keskusmuisti	2 GB RAM
Vaadittava levytila	• Forefront Endpoint Protection Server: 600 Mb • Forefront Endpoint Protection tietokanta: 1,25 Gb • Forefront Endpoint Protection reporting tietokanta: 1,25 Gb
Käyttöjärjestelmä	• Windows Server® 2003 Standard, Enterprise, tai Datacenter Edition Service Pack 2 (x86 tai x64) • Windows Server 2008 Standard, Enterprise, tai Datacenter Service Pack 1 (x86 tai x64) • Windows Server 2008 R2 Standard, Enterprise, tai Datacenter (x64)
Tietokantapalvelimet	• Microsoft SQL Server 2005 Standard tai Enterprise Edition Service Pack 3 (x86 tai x64) • Microsoft SQL Server 2008 Standard tai Enterprise (x86 tai x64) • Microsoft SQL Server 2008 R2 Standard tai Enterprise (x86 tai x64)
Lisävaatimukset Forefront Endpoint Protection reporting -tietokannan asentamiseen	• SQL Server Analysis Services • SQL Server Integration Services • SQL Server Reporting Services

	• SQL Server Agent
Lisävaatimukset Forefront Endpoint Protection reporting -tietokannan asentamiselle SQL-Server-klusteriin	• Nimi, jonka laitoit **SQL network name** kohtaan SQL Server klusterille, täytyy olla rekisteröity toimialueelle • SQL Server Integration Services täytyy olla asennettuna jokaiselle nodelle ja kuulua klusteriryhmään
Configuration Manager	• Microsoft System Center Configuration Manager 2007 Service Pack 2 asennettu oletusrooleilla, sekä: - Microsoft System Center Configuration Manager 2007 R2 asennettu ja konfiguroitu käyttämään SQL Server Reporting Services - Microsoft System Center Configuration Manager 2007 R3 asennettu ja konfiguroitu käyttämään SQL Server Reporting Services • Seuraavat client agentit ovat asennettuna ja konfiguroituna: - Hardware Inventory - Software Distribution - Desired Configuration Management
Lisävaatimukset	• Ei muita Forefront Endpoint Protection versioita asennettuna • Microsoft Windows Installer versio 3.1 • Microsoft .Net Framework 3.5 Service Pack 1 • Configuration Manager Hotfix KB2271736 (http://go.microsoft.com/fwlink/?LinkId=203936) • SQL Server Analysis Management Objects • Tietokone, johon asennus suoritetaan, ei vaadi uudelleen käynnistystä edellisestä asennuksesta tai päivityksestä • Asennuksen suorittava käyttäjä on sen toimi-

	alueen domainkäyttäjä, jossa Forefront Endpoint Protection palvelin sijaitsee
Hallintakonsolin laitteistovaatimukset	
Configuration Manager	• Microsoft System Center Configuration Manager 2007 Service Pack 2 Console • Microsoft System Center Configuration Manager 2007 R2 • Microsoft System Center Configuration Manager 2007 R3
Lisävaatimukset	• Microsoft .Net Framework 3.5 Service Pack 1 • Configuration Manager Hotfix KB2271736 (http://go.microsoft.com/fwlink/?LinkId=203936) • Tietokone, johon asennus suoritetaan, ei vaadi uudelleen käynnistystä edellisestä asennuksesta tai päivityksestä • Asennuksen suorittava käyttäjä on sen toimialueen domainkäyttäjä, jossa Forefront Endpoint Protection palvelin sijaitsee
Asiakastietokoneen laitteistovaatimukset	
Configuration Manager	Microsoft System Center Configuration Manager 2007 saitille on Forefront Endpoint Protection server asennettu.
Käyttöjärjestelmä	• Windows 7 (x86 tai x64) • Windows 7 XP mode • Windows Vista (x86 tai x64) tai uudempi • Windows XP Service Pack 2 (x86 tai x64) tai uudempi • Windows Server 2008 R2 (x64) tai uudempi • Windows Server 2008 R2 Server Core (x64) • Windows Server 2008 (x86 tai x64) tai uudempi

	• Windows Server 2003 Service Pack 2 (x86 tai x64) tai uudempi • Windows Server 2003 R2 (x86 tai x64) tai uudempi Voit asentaa asiakasohjelman seuraaviin käyttöjärjestelmiin ja hallita niiden sääntöjä, mutta asiakastietokone ei pysty lähettämään tietoa Forefront Endpoint Protection hallintapaneelille. • Windows Server 2008 Server Core (x86 tai x64) Älä ota käyttöön File-based tai Enhanced Write suodattimia seuraavilla käyttöjärjestelmille. • Windows Embedded Standard 7 SP1 images based on the FEP 2010 dependency template • Windows Embedded POSReady 7 • Windows ThinPC
Vaadittava levytila	255 MB
Lisävaatimukset	• Windows Installer 3.1 tai uudempi • Secondary Logon service täytyy olla päällä • Filter manager rollup package for Windows XP Service Pack 2 (x86) KB914882 (http://go.microsoft.com/fwlink/?LinkID=207000)

Kuten vaatimuksista voi huomata, FEP 2010 toimii laajalla valikoimalla eri kokoonpanoja. Kokoonpanot, joita käytettiin asennuksessa Helsingin palvelualojen oppilaitoksessa, olivat vaatimuksien mukaiset (taulukko 3), mutta puutteita oli muun muassa palvelimien ohjelmistokomponenttien kanssa ja päivityksissä.

Taulukko 3. Projektissa käytettävien virtuaalipalvelimien tiedot.

Palvelin	SCCM	SQL
Suoritin	AMD Phenom 9350e 1,9 GHz	AMD Opteron 2347 HE 1,9 GHz
Keskusmuisti	3 GB	8 GB
Käyttöjärjestelmä	Windows Server 2003 Standard (R2) 32-bit	Windows Server 2008 Enterprise (R2) 64-bit
Muuta	Microsoft Configuration Manager 2007 (R3)	Microsoft SQL-Server 2008 (R2)

Kun laitteistovaatimukset on selvitetty ja tarvittavat puutteet lisätty omaan palvelinjärjestelmään, voidaan aloittaa suunnittelu ja tarvittavat aloitustoimenpiteet. Seuraavaksi käsitellään kyseiseen projektiin käytetty asennusmalli ja käydään läpi vaadittavien lisäroolien asennus palvelimille.

4.2 Suunnittelu ja aloitustoimenpiteet

Projektiin käytettiin perusasennusta etäraportointitietokannan kanssa (taulukko 4). (8.) Kyseisessä mallissa FEP 2010 asennetaan tietoverkon käyttämälle SCCM-palvelimelle ja se konfiguroidaan käyttämään erillisen SQL-palvelimen raportointitietokantoja.

Taulukko 4. Asennuskomponenttien sijainnit perusasennuksessa etäraportointitietokannan kanssa. (lähde)

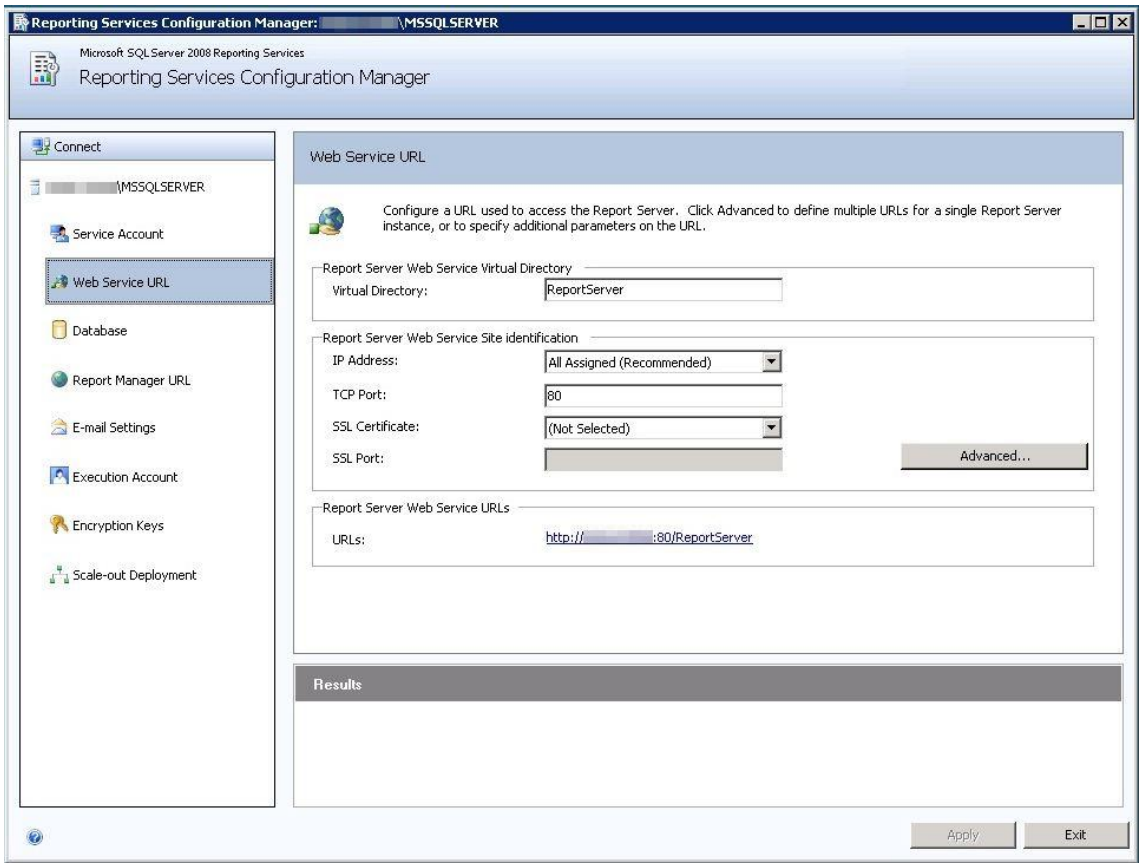
Asennuskomponentit	**Mihin asennetaan**
Forefront Endpoint Protection tietokanta	SQL-palvelimelle ja samaan instanssiin Configuration Manager tietokannan kanssa.
Forefront Endpoint Protection Site-palvelin laajennokset Configuration Managerille.	SCCM-palvelimelle
Forefront Endpoint Protection konsolilaajennukset Configuration Managerille.	SCCM-palvelimelle
Forefront Endpoint Protection raportointirooli	SQL-palvelimelle
Forefront Endpoint Protection raportointitietokanta	SQL-palvelimelle

Ensimmäinen toimenpide on tarkistaa mahdolliset ohjelmistopäivitykset, jotka puuttuivat projektin palvelimilta. Asennustöiden sujuvuuden kannalta päivitykset tulisi asentaa ennen muita toimenpiteitä. Näihin kuuluivat hotfix, joka antaa lisätuen Management Class -luokille SCCM-palvelimelle, sekä Microsoft analysis management objects -päivitys. Tarvittavat asennustiedostot löytyvät Microsoftin päivityssivustoilta http://support.microsoft.com/kb/2271736 ja http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=3522. Seuraavaksi käydään läpi mahdollisesti puuttuvien palvelinkomponenttien asentaminen.

4.3 Puuttuvien palvelinkomponenttien lisääminen

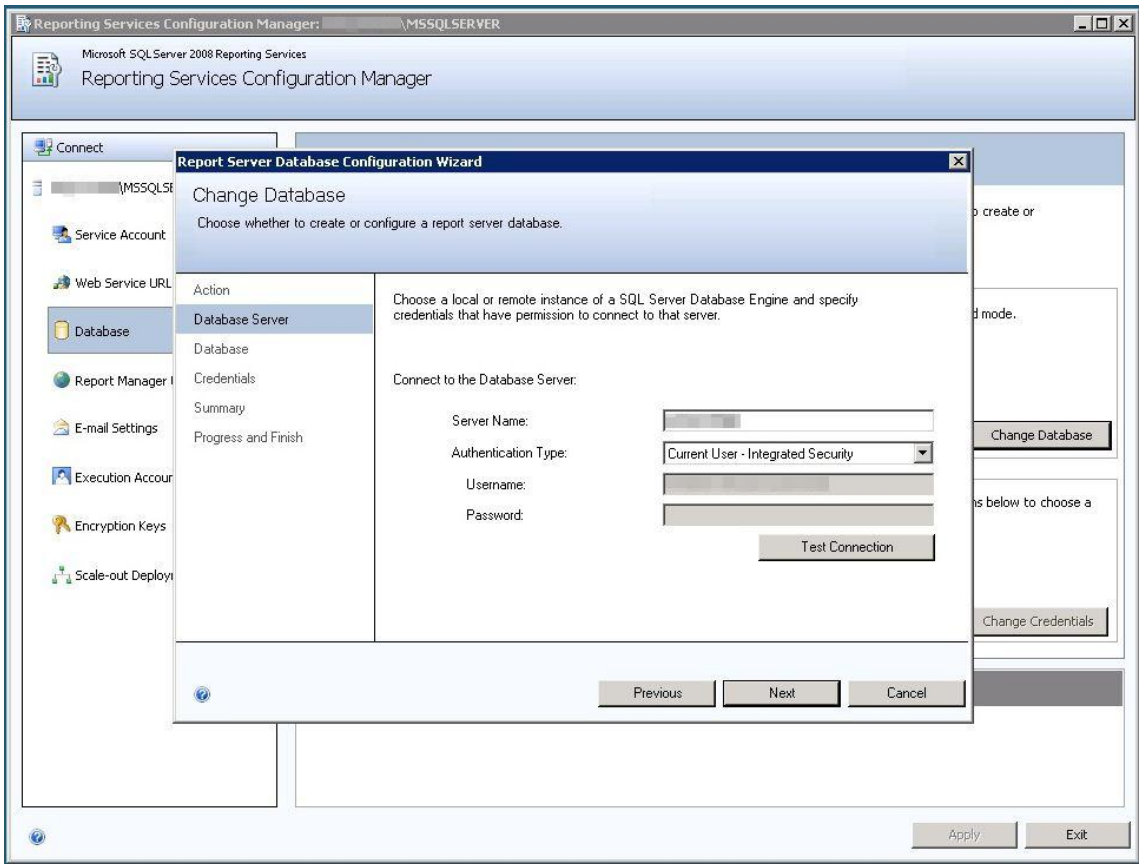
Projektissa käytetyltä SQL-palvelimelta puuttuivat Reporting Services-, Integration Services- ja Analysis Services-palvelinkomponentit, joten ne täytyi ottaa käyttöön ennen FEP 2010:n asentamista. Itse lisäkomponenttien asentaminen on varsin suoraviivaista työtä. Aluksi mennään hallintapaneeliin, josta seuraavaksi programs and features -valikkoon. Valitaan sieltä Microsoft SQL-server 2008 (tai vastaava, joka on käytössä) ja klikataan uninstall/change. Eteen tulevasta ikkunasta valitaan add, jonka kautta voi lisätä olemassa olevaan asennukseen komponentteja. Seuraavana asennus kysyy, mihin instanssiin ja tietokantaan halutaan tehdä muutoksia. Valitaan sama instanssi ja tietokanta, jolle aiotaan asentaa FEP 2010. Tämän jälkeen asennuksen ohjeita seuraamalla voidaan lisätä Reporting Services, Integration Services ja Analysis Services -komponentit.

Asennuksen jälkeen Integration Services ja Analysis Services eivät todennäköisesti vaadi mitään lisätoimenpiteitä FEP 2010:tä varten, mutta Reporting Services täytyy konfiguroida ennen käyttöä. Asetuksia varten avaa Reporting Services Configuration Manager. Web Service URL -valikossa määritellään palvelun käyttämä URL-osoite. Suositeltavaa on käyttää oletusarvona annettua ReportServer-virtuaalikansiota (kuva 2). IP-osoite, TCP-portti ja SSL-sertifikaatti -asetukset voidaan määritellä tarpeiden mukaan. Report Manager URL -valikko on varsin samanlainen, jossa kannattaa myös pitää tarjottu oletus-URL-osoite.



Kuva 2. Reporting Services Configuration Manager Web Service -valikko.

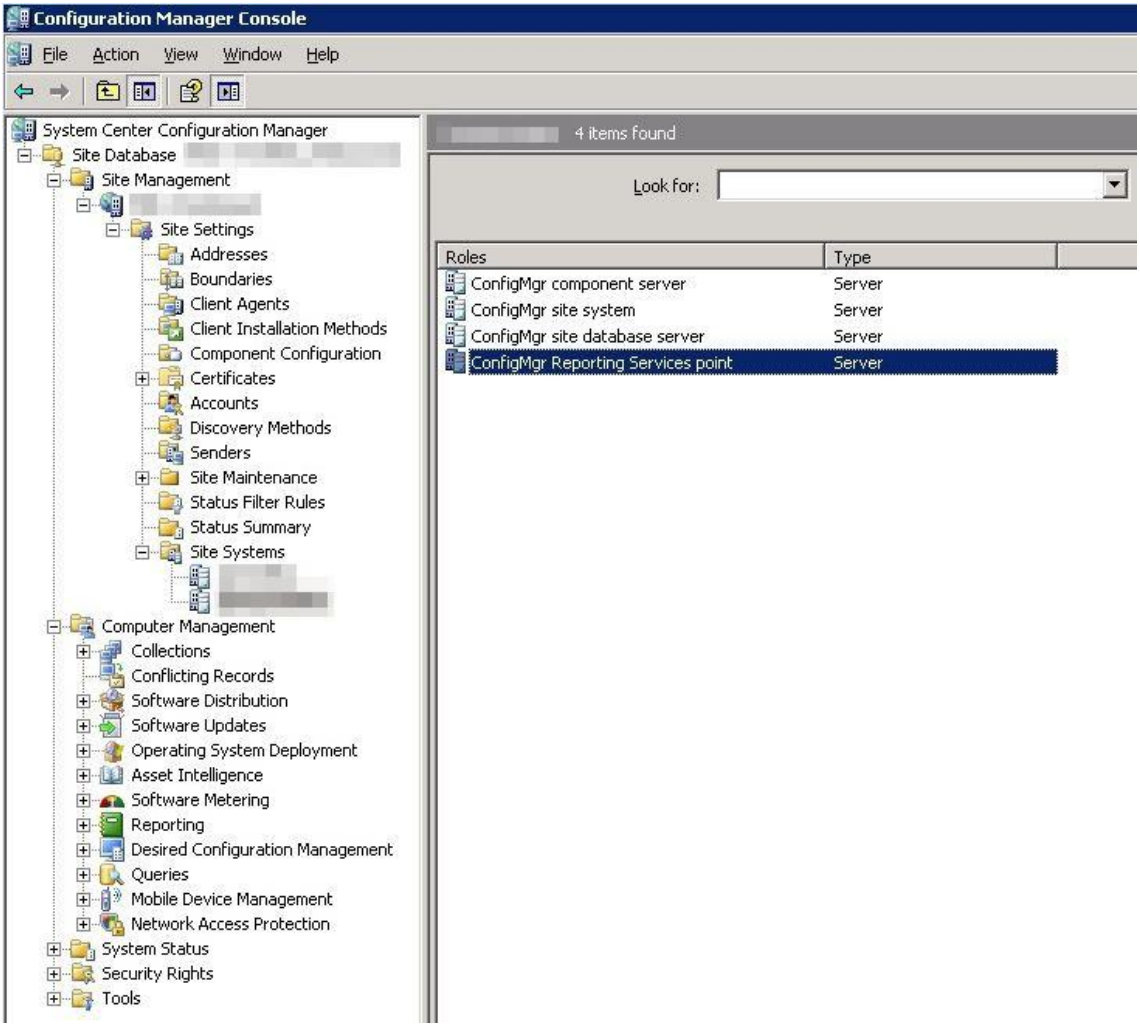
Database -valikossa määritellään Reporting Services -palvelun käyttämä palvelin ja tietokanta (kuva 3). Projektissa käytettiin palvelimena nykyistä SQL-palvelinta. Muut asetukset tulee valita tapauskohtaisesti jokaisen verkon kohdalla. Nimettyjä instansseja ei tulisi käyttää, jos mahdollista. Muita Reporting Services Configuration Managerin asetuksia joihin, kuuluivat e-mail settings, encryption keys ja scale-out deployment, ei ollut tarpeen asettaa projektia varten.



Kuva 3. Reporting Services Configuration Manager Database -valikko.

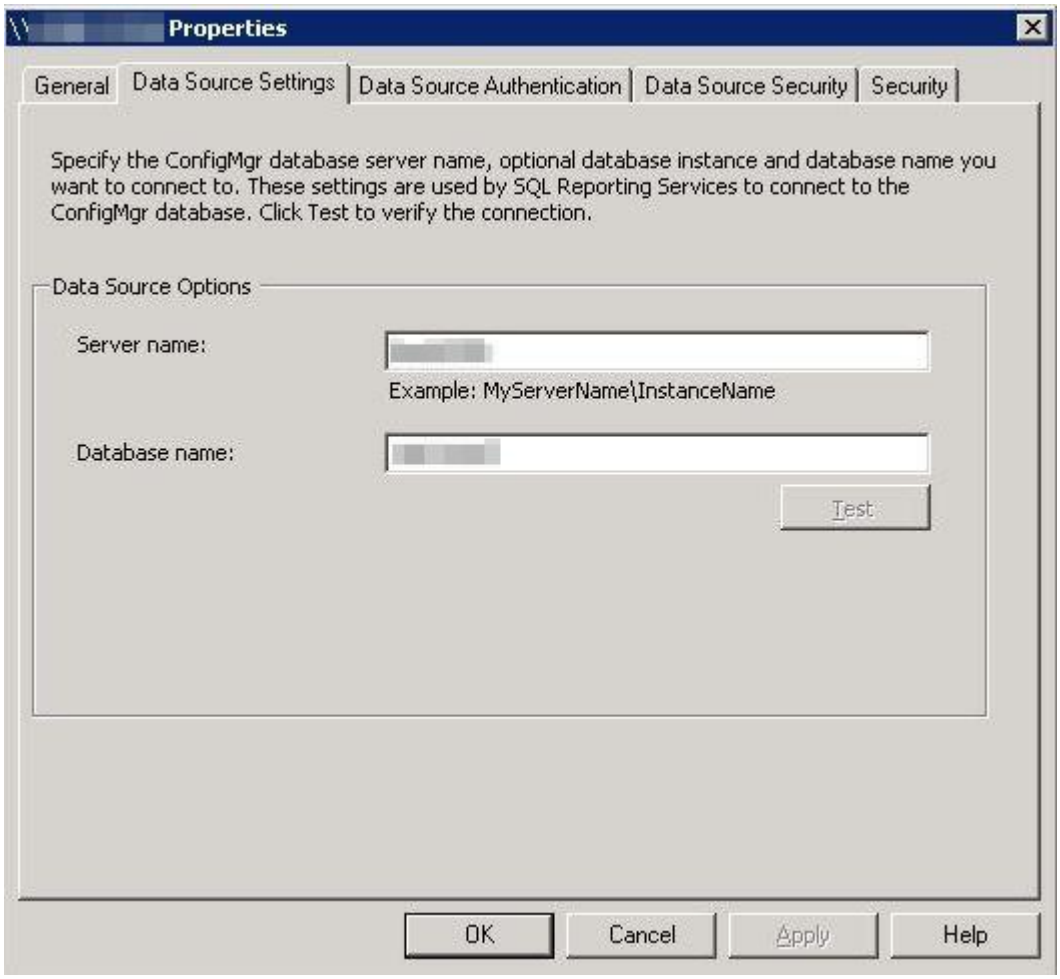
Kun tarpeelliset asetukset on tehty, niin kannattaa yrittää mennä raportointisivuille käyttämällä URL-osoitteita, jotka annettiin Reporting Services Configuration Managerille. URL-osoitteet ovat muotoa http://<palvelimen_nimi>/Reports ja http://<palvelimen_nimi>/ReportServer. Jos yhteys saadaan molempiin osoitteisiin, niin reporting services mitä todennäköisemmin on toimintakunnossa.

Kun yhteys toimii, mennään SCCM-palvelimelle ja avataan Microsoft Configuration Manager konsoli. Seuraavaksi lisätään Reporting Services point –rooli palvelimelle, jotta SCCM-palvelin pystyy käsittelemään SQL-palvelimen lähettämiä raportointitietoja. Roolin voi lisätä menemällä Site database -> Site management -> <palvelimen_nimi> -> Site settings -> Site systems. Tämän jälkeen klikaataan oikealla hiirennäppäimellä SQL-palvelinta ja esille tulevasta valikosta valitaan new roles. Asennuksen ohjeita seuraamalla voidaan lisätä tarvittavan Reporting Services Point -roolin. Sen pitäisi näkyä asennuksen jälkeen rooliluettelossa (kuva 4).



Kuva 4. Reporting Services pointin sijainti Configuration Managerissa.

Tämän jälkeen täytyy vielä laittaa asetukset kuntoon Reporting Services point –roolille. Mennään Site management -> Computer management -> Reporting -> Reporting services, jonka alta löytyy asennettu raportointipalvelu. Klikataan palvelua hiiren oikealla näppäimellä ja valitse eteen tulevasta valikosta properties (kuva 5). Syötetään tarvittavat tiedot tyhjiin kenttiin, jonka jälkeen voidaan kopioida olemassa olevat raportit valitsemalla copy reports to reporting services samasta kontekstivalikosta.



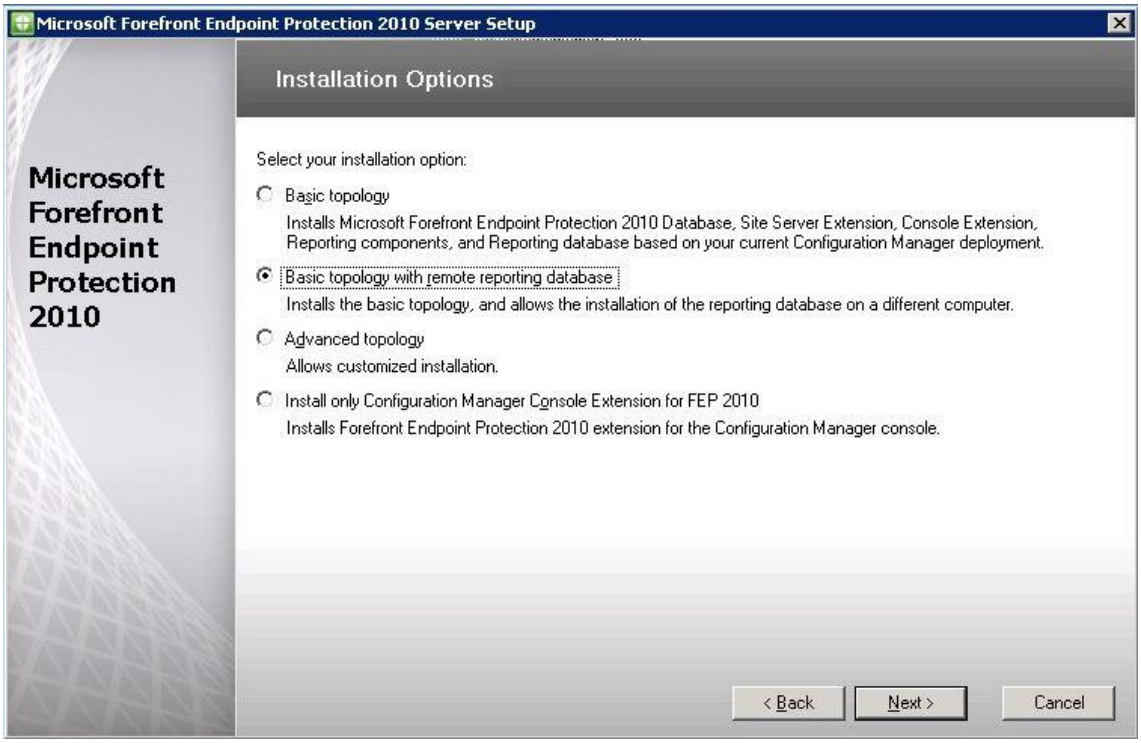
Kuva 5. Raportointipalvelun ominaisuusasetukset.

Reporting Services:in pitäisi nyt olla toiminnassa, mikä oli projektin suurin este FEP 2010:n asentamiselle. Analysis Services:in ja Integration Services:in tulisi toimia ilman lisätoimenpiteitä, eivätkä näin ole esteenä jatkoasennuksille. Kun kaikki vaadittavat komponentit ja päivitykset on asennettu, voidaan siirtyä itse FEP 2010:n asentamiseen. Pitää muistaa, että puutteet eivät ole välttämättä samat muissa kokoonpanoissa.

4.4 FEP 2010:n palvelinasennus

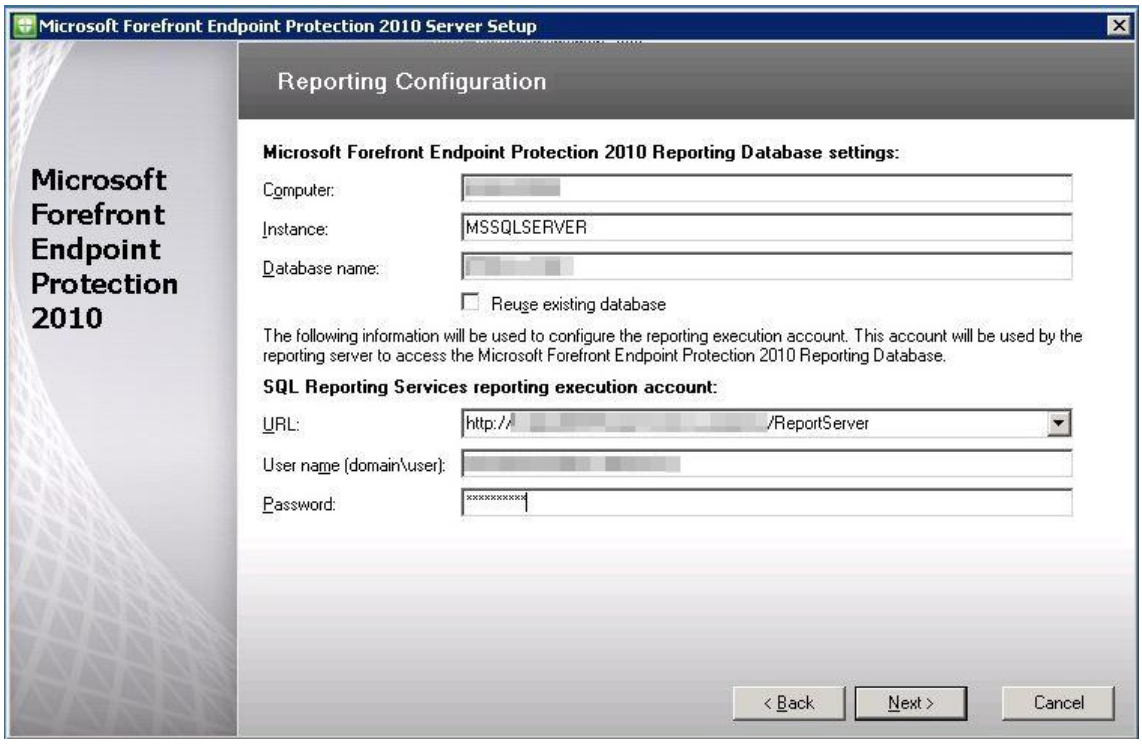
Tässä vaiheessa pitäisi olla kaikki vaadittavat alkutoimenpiteet tehtynä, jolloin voidaan aloittaa FEP 2010 -tietoturvapalvelun asentaminen SCCM-palvelimelle. Riippuen mikä käyttöjärjestelmä palvelimella on, valitaan sen mukaan, asennetaanko 32- vai 64-bittisen versio. Projektissa oli palvelimella käytössä 32-bittinen Microsoft Windows Server 2003 käyttöjärjestelmä, joten asennukseen käytettiin sen mukaisesti 32-bittistä

asennustiedostoa. Asennuksen alussa kysytään, mitä topologiaa halutaan käyttää (kuva 6). Projektille valittiin Basic topology with remote reporting database -kohta, koska SQL-palvelin on erillinen SCCM-palvelimesta, jolloin raportointitietokannat sijaitsevat eri tietokoneella.



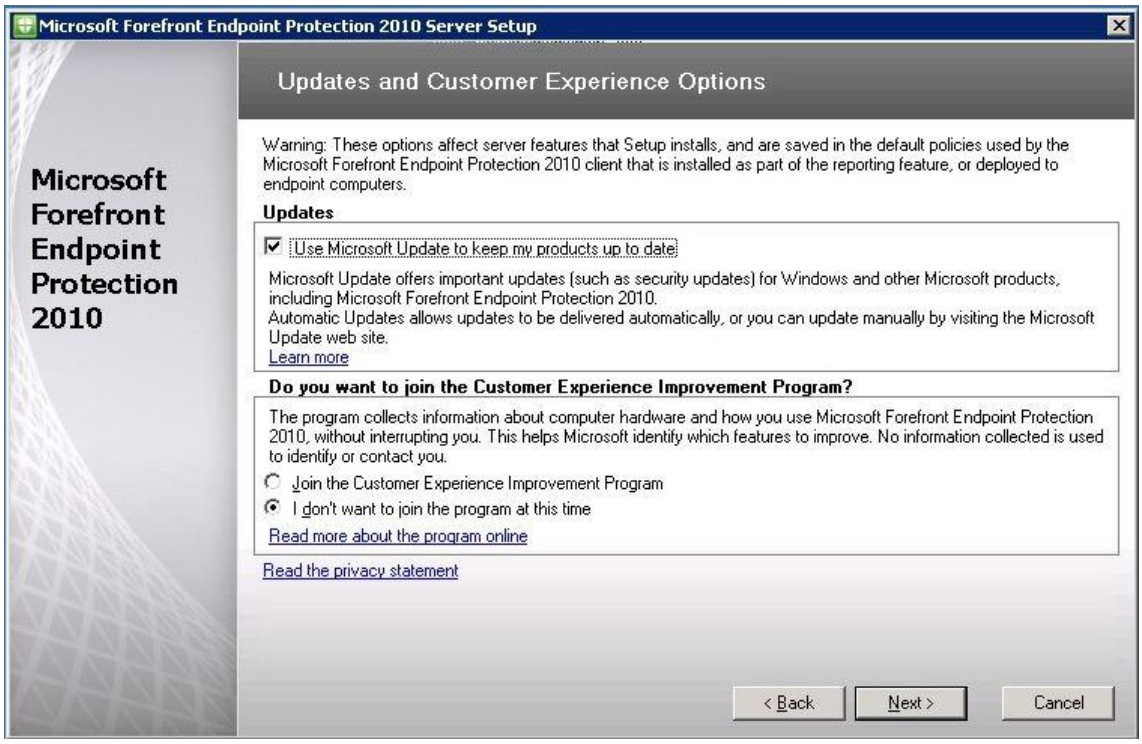
Kuva 6. FEP 2010 asennuksen topologian valinta.

Seuraavassa asennuksen vaiheessa tulee antaa tarvittavat tiedot koskien raportointitietokantaa (kuva 7). Näihin kuuluvat palvelimen nimi, instanssi, tietokannan nimi ja Reporting Services URL-osoite. Lopuksi tulee myös määrittää käyttäjä ja salasana.



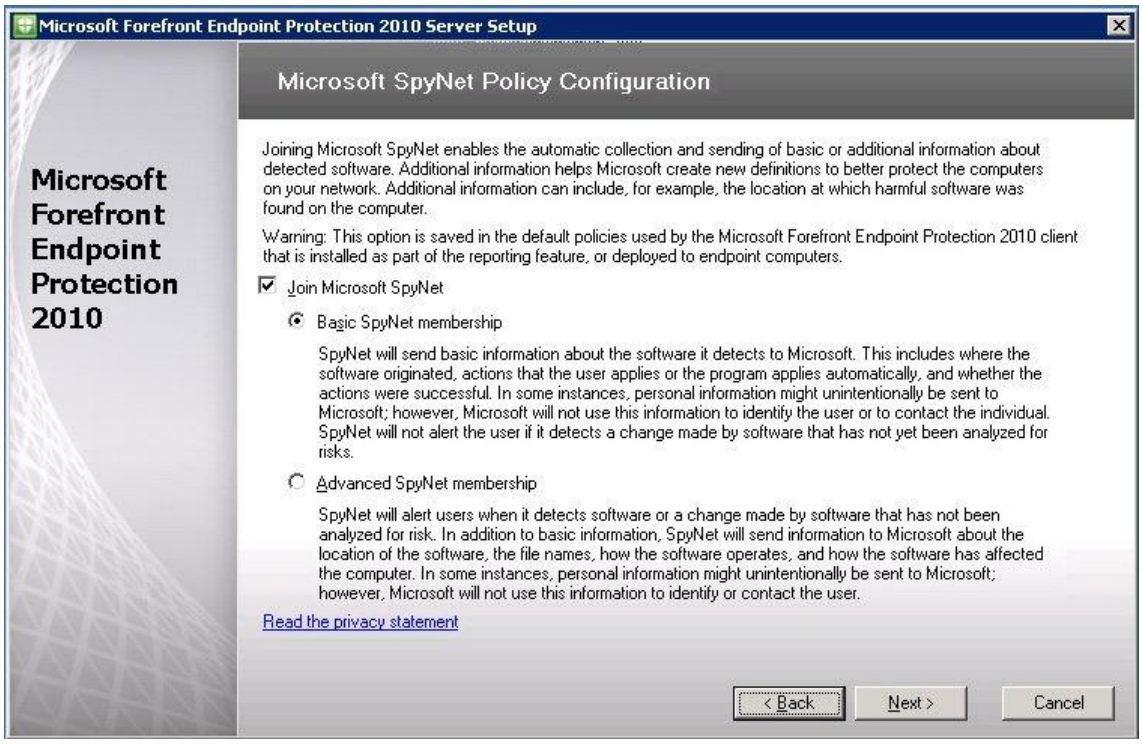
Kuva 7. FEP 2010 asennuksessa tarvittavien tietojen lisääminen.

Asetuksien määrittämisen jälkeen asennus kysyy, käytetäänkö päivityksien lataamiseen Microsoft Update -palvelua sekä liitytäänkö Customer Experience Improvement Program -palveluun (kuva 8). Projektille valittiin päivityksien asentaminen ja jälkimmäiseen jätettiin liittymättä. Microsoft Update –palvelun käyttäminen on suositeltavaa, mutta sen käyttö riippuu, minkälaiseen ympäristöön ohjelma asennetaan.



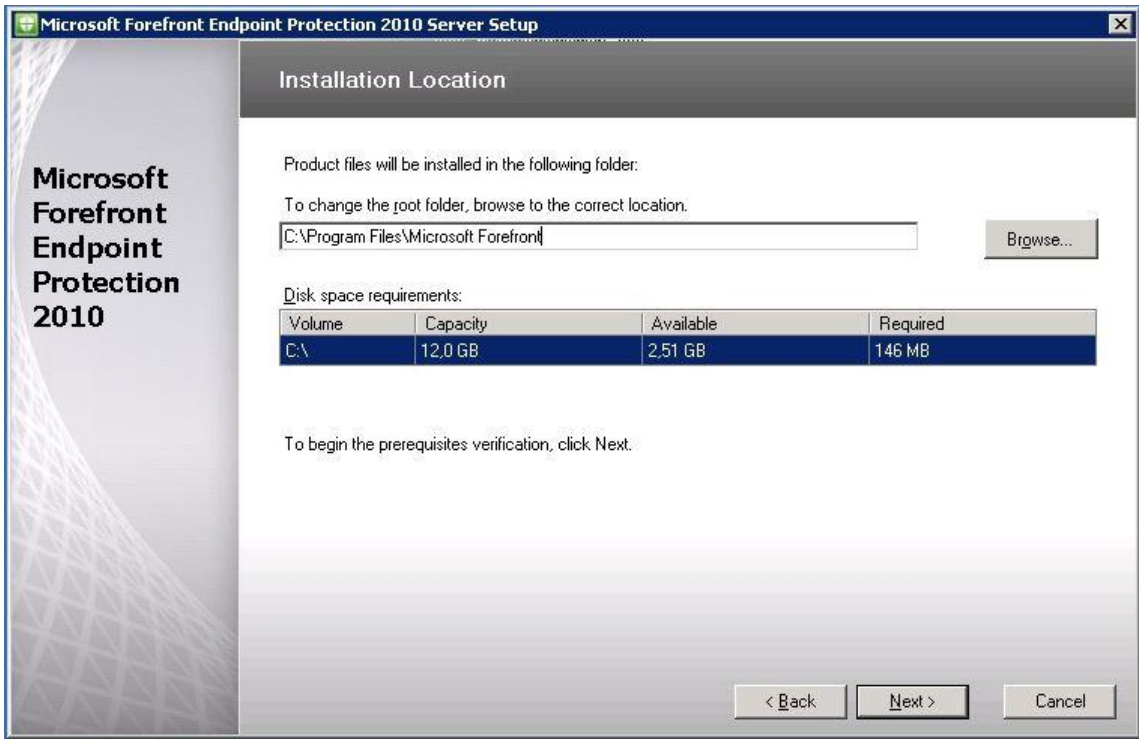
Kuva 8. FEP 2010 asennukseen liittyvät lisäpalvelut.

Seuraavaksi asennus kysyy liittymisestä Microsoft SpyNetiin (kuva 9). Kyseessä on palvelu, joka lähettää anonyymiä tietoa eri haittaohjelmista FEP 2010 mahdollisesti löytää. Tämä muun muassa parantaa ja nopeuttaa uusien virustietokantapäivityksien laatua. Projektissa liityttiin palveluun, koska siitä on pelkästään hyötyä tietoturvan kannalta.



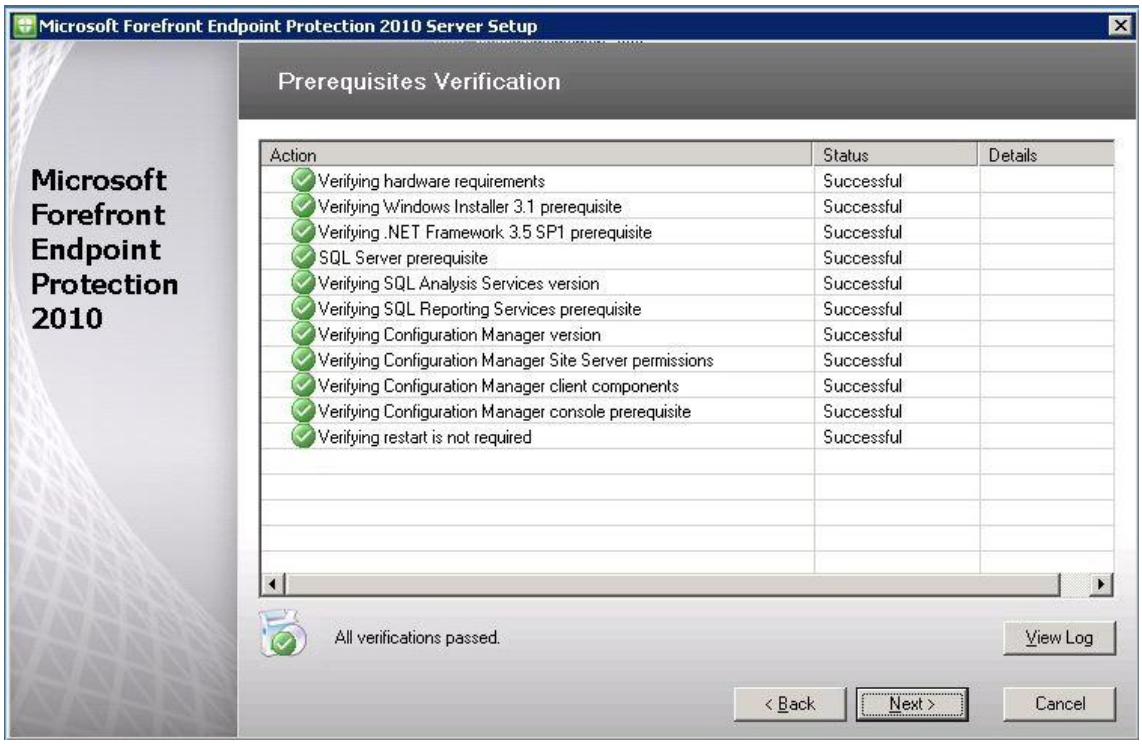
Kuva 9. FEP 2010:n asennus kysyy Microsoft SpyNetiin liittymisestä.

Lopuksi asennus pyytää, mihin kansioon FEP 2010 asennetaan, ja informoi mahdollisesta tilan puutteesta kovalevyllä (kuva 10). Projektissa asennukselle käytettiin oletuskansiota. FEP 2010 ei vie paljoa tilaa, joten tässä vaiheessa ei pitäisi tulla ongelmia vastaan.



Kuva 10. FEP 2010 asennus pyytää asennuskansiota.

Kun kaikki asennuksen muut vaiheet on suoritettu, tarkistetaan ovatko kaikki FEP 2010:n tarvitsemat lisäohjelmistot, päivitykset ja komponentit asennettuina (kuva 11). Projektin tässä vaiheessa tuli aluksi virhe, koska pari päivitystä puuttui. Tämän vaiheen vuoksi asennustyöntekijän tulisi olla tarkkana, jotta kaikki tarvittavat puutteet ovat asennettuina. Jos kaikki kohdat on merkitty kunnossa olevaksi, niin asennuksen tulisi onnistua.



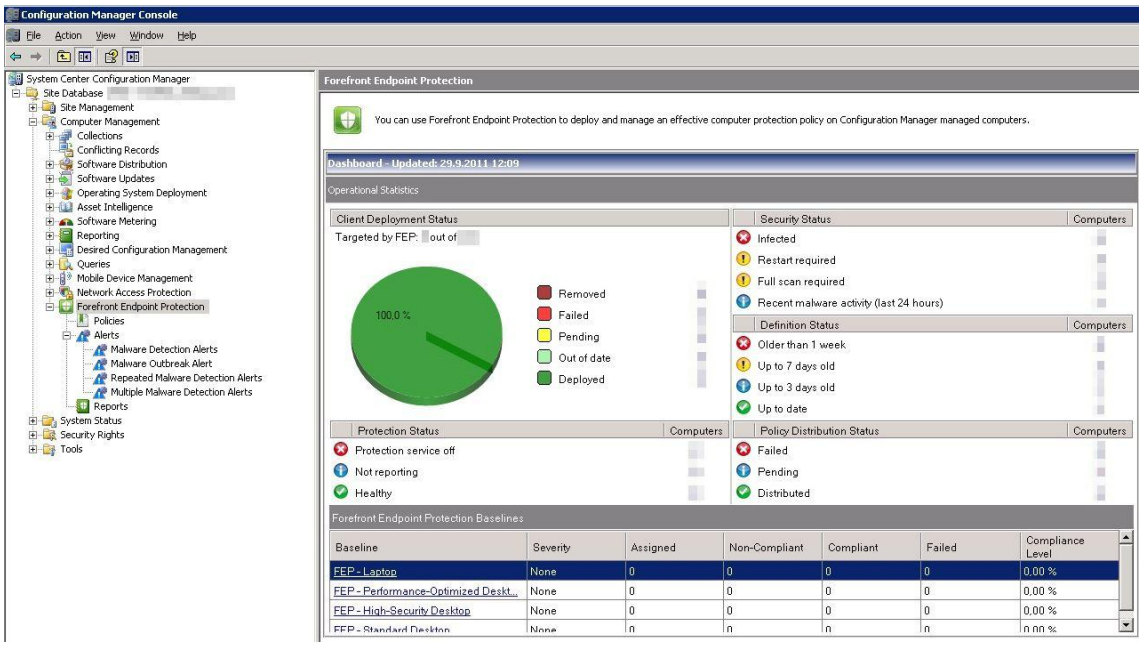
Kuva 11. FEP 2010:n asennus tarkistaa tarpeelliset puutteet.

Asennuksen jälkeen pitäisi Microsoft Configuration Managerissa olla näkyvissä Forefront Endpoint Protection -valikko. Se löytyy menemällä Site Database -> Computer Management -> Forefront Endpoint Protection. Valikosta löytyy muun muassa FEP 2010:n hallintapaneeli. FEP 2010:n hallintapaneelia ja asetuksia käsitellään seuraavissa luvussa tarkemmin.

FEP 2010:n käsiasennus asiakas-tietokoneisiin on hyvin suoraviivainen toimenpide. Käsiasennus kannattaa tehdä testiryhmälle tietokoneita, ennen kuin levittää tuotetta Microsoftin Configuration Managerilla isommalle määrälle laitteita. Asennusvaiheessa kysytään liittymisestä Microsoftin Spynet-palveluun kuten palvelinasennuksessa, sekä käytetäänkö Windows-palomuuria. Asennuksen jälkeen tietokoneen tulisi näkyä FEP 2010 hallintapaneelissa SCCM-palvelimella.

5 Ylläpito FEP 2010:n hallintapaneelilla

Forefront Endpoint Protection 2010:n hallinta onnistuu täysin Configuration Managerin kautta, koska tuote on täysin integroitu käyttämään kyseistä hallinta-arkkitehtuuria. FEP 2010:n hallintapaneeli tarjoaa yleisnäkymän tietoverkon FEP 2010:llä suojattujen tietokoneiden tiloista (kuva 12). Näkyvissä on esimerkiksi piirakkadiagrammi, josta näkee heti tietoverkon FEP 2010:llä turvattujen tietokoneiden tilat. Paneelista näkee myös heti mahdollisesti saastuneiden tietokoneiden lukumäärän ja uusien viruspäivityksien tilat eri tietokoneilla.



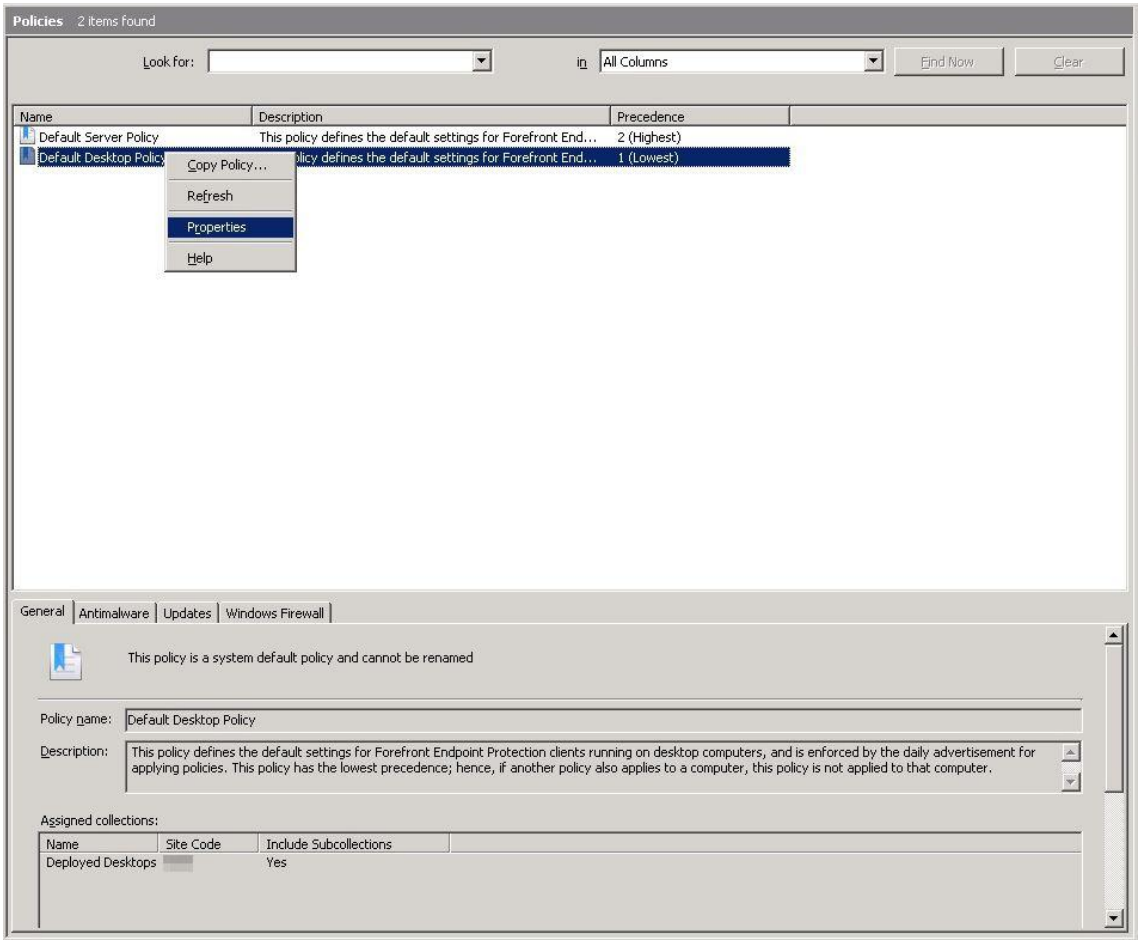
Kuva 12. Yleiskuva FEP 2010:n hallintapaneelista.

Klikkaamalla eri tapahtumien lukumääriä hallintapaneelissa pääsee suoraan FEP 2010:n tapahtumaa koskevaan kokoelmaan tietokoneita. Tämä helpottaa mahdollisen laitteen löytämistä isommastakin tietoverkosta. Seuraavaksi katsotaan tarkemmin hallintapaneelin tärkeimpiä ominaisuuksia, joihin kuuluvat toimintaohjeet eri tietokoneille sekä hälytykset ja raportit.

5.1 Toimintaohjeet

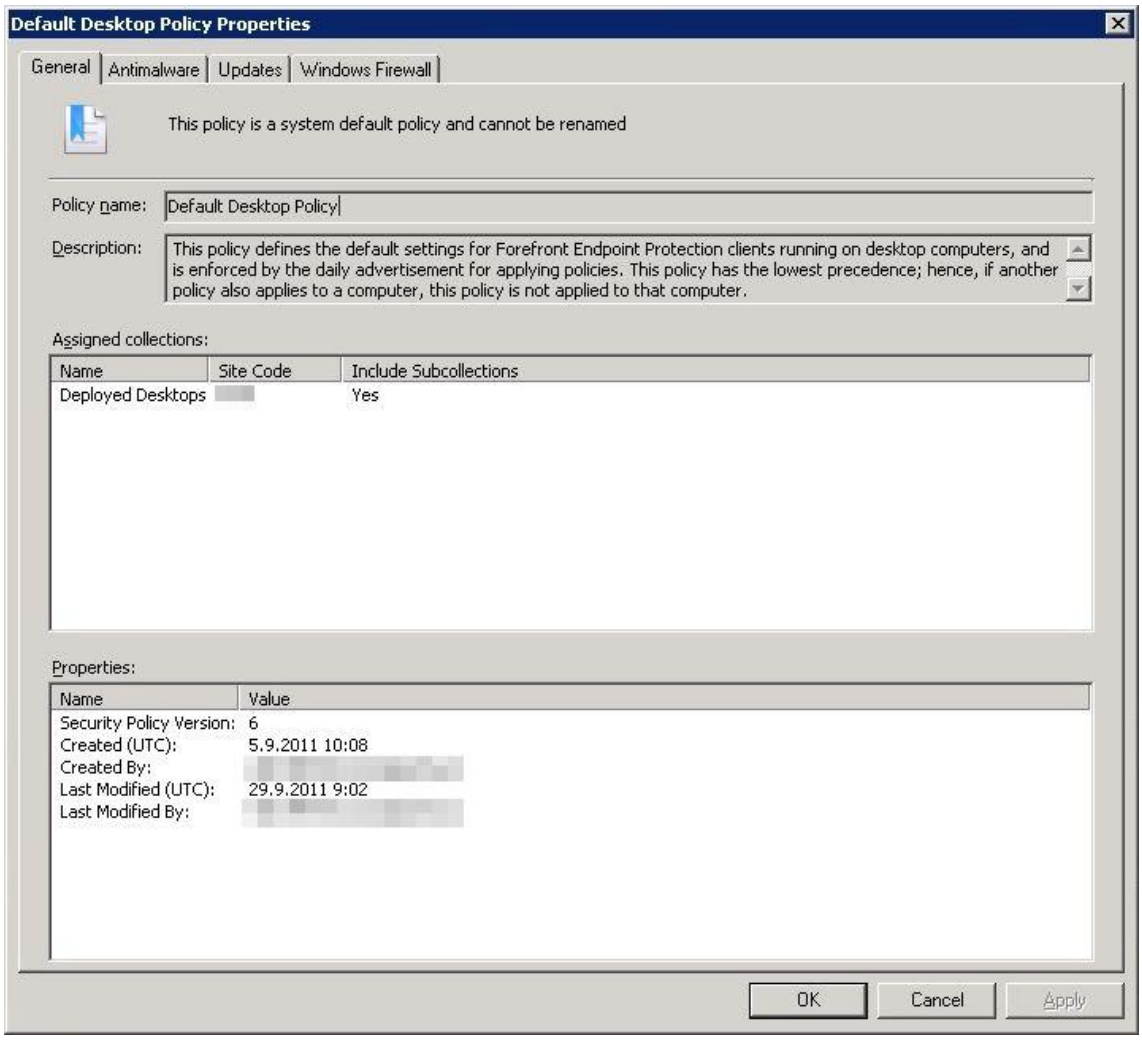
FEP 2010:n toimintaohjeisiin pääsee menemällä Site Database -> Computer Management -> Forefront Endpoint Protection -> Policies. Toimintaohjeet palvelin- ja asiakas-

koneille ovat valmiina oletuksena, mutta uusia on mahdollista lisätä tai oletusasetuksia muokata. Projektissa ei ollut tarvetta tehdä uusia toimintaohjeita. Tarvetta oli vain muokata olemassa olevien toimintaohjeiden asetuksia. Asetuksia pääsee muokkaamaan valitsemalla hiiren oikealla haluama oletustoimintaohje ja kontekstivalikosta valitsemalla Properties-kohta (kuva 13).



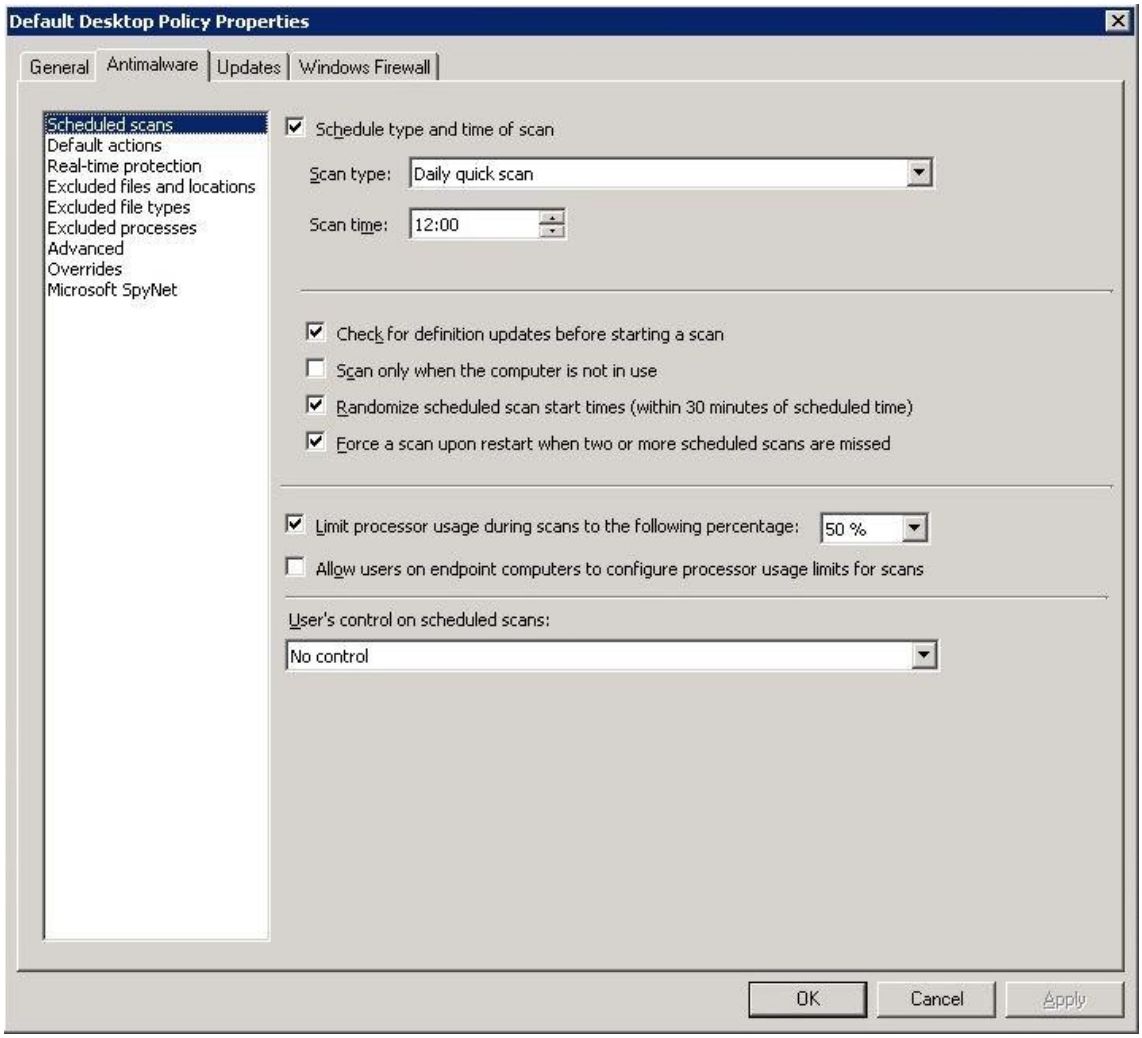
Kuva 13. FEP 2010:n toimintaohjevalikko.

Asetuksista löytyvät General, Antimalware, Updates ja Windows Firewall -välilehdet. Ensimmäisenä mennään General-välilehdelle (kuva 14), josta näkee, mihin tietokonekokoelmiin kyseistä toimintaohjetta jaetaan. Lisäksi sivulta näkee, mikä on toimintaohjeen versio ja milloin se on tehty. Tällä välilehdellä ei ole mitään muokattavaa, jos valitaan oletustoimintaohje.



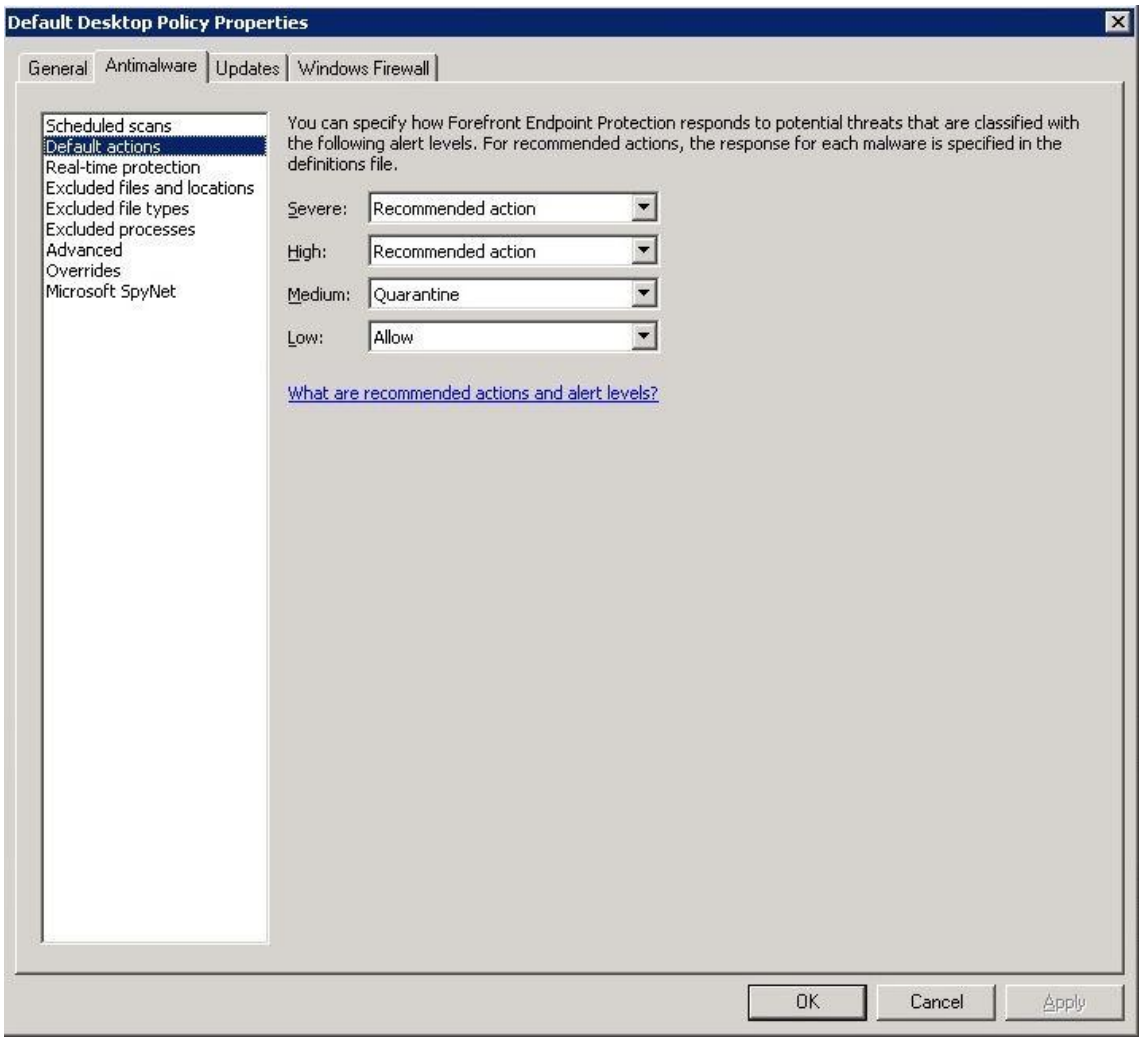
Kuva 14. Toimintaohjeasetuksien General-välilehti.

Asetuksien Antimalware-välilehdeltä löytyy suurin osa tarpeellisista asetuksista. Näistä ensimmäisenä Scheduled scans -asetukset (kuva 15), jossa voi muokata aikoja, jolloin tietokoneiden virus-skannaaminen tapahtuu. Mahdollista on myös muun muassa asettaa viruspäivitykset tulemaan ennen skannausta, jolloin skannaus tapahtuu uusimpien virustietokantojen pohjalta. Skannausaikoja voi myös satunnaistaa, joka vähentää tietoliikennekuormaa isoissa tietoverkoissa. Jos jotkin tietokoneet eivät esimerkiksi ole päällä skannauksen aikana, voi asettaa pakotetun skannauksen, joka tapahtuu seuraavan käynnistyskerran yhteydessä. Tärkeänä asetuksena on myös suoritinkäytön rajoittaminen skannauksen aikana, jotta virustorjunta ei haittaisi käyttäjän työskentelyä. Lopuksi voi vielä määritellä, annetaanko käyttäjälle oikeus muuttaa skannausasetuksia. Suositeltavaa olisi rajoittaa käyttäjien oikeuksia mahdollisimman paljon tietoturvariskien takia.



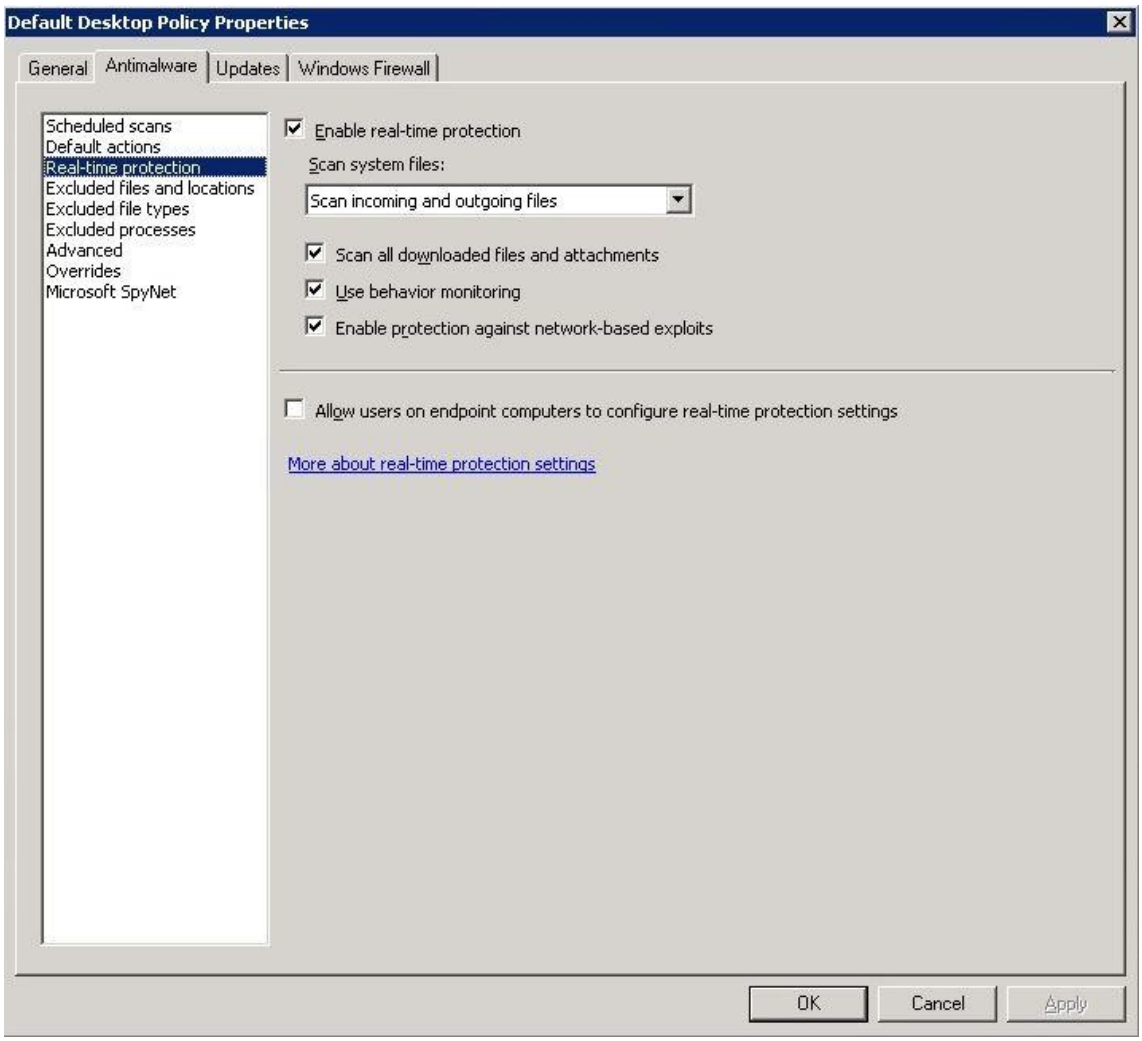
Kuva 15. Antimalware-välilehden Scheduled scans -asetukset.

Seuraavana on Default actions -asetukset (kuva 16), joissa määritellään oletustoimenpiteet eri tason uhille. Valikosta voi valita suositellut toimenpiteet, karanteeni tai salliminen eri tason tietoturvauhille. Näistä harmittomin Low-uhkataso vastaa lähinnä tarpeetonta ohjelmaa tietokoneella, josta ei ole välitöntä tietoturvariskiä. Taas Severe-uhkataso vastaa välitöntä tietoturvariskiä. On suositeltavaa pitää Recommended actions -kohta valittuna, koska tällöin FEP 2010 valitsee parhaan mahdollisen toimenpiteen löydetyn haittaohjelman mukaan. (9.)



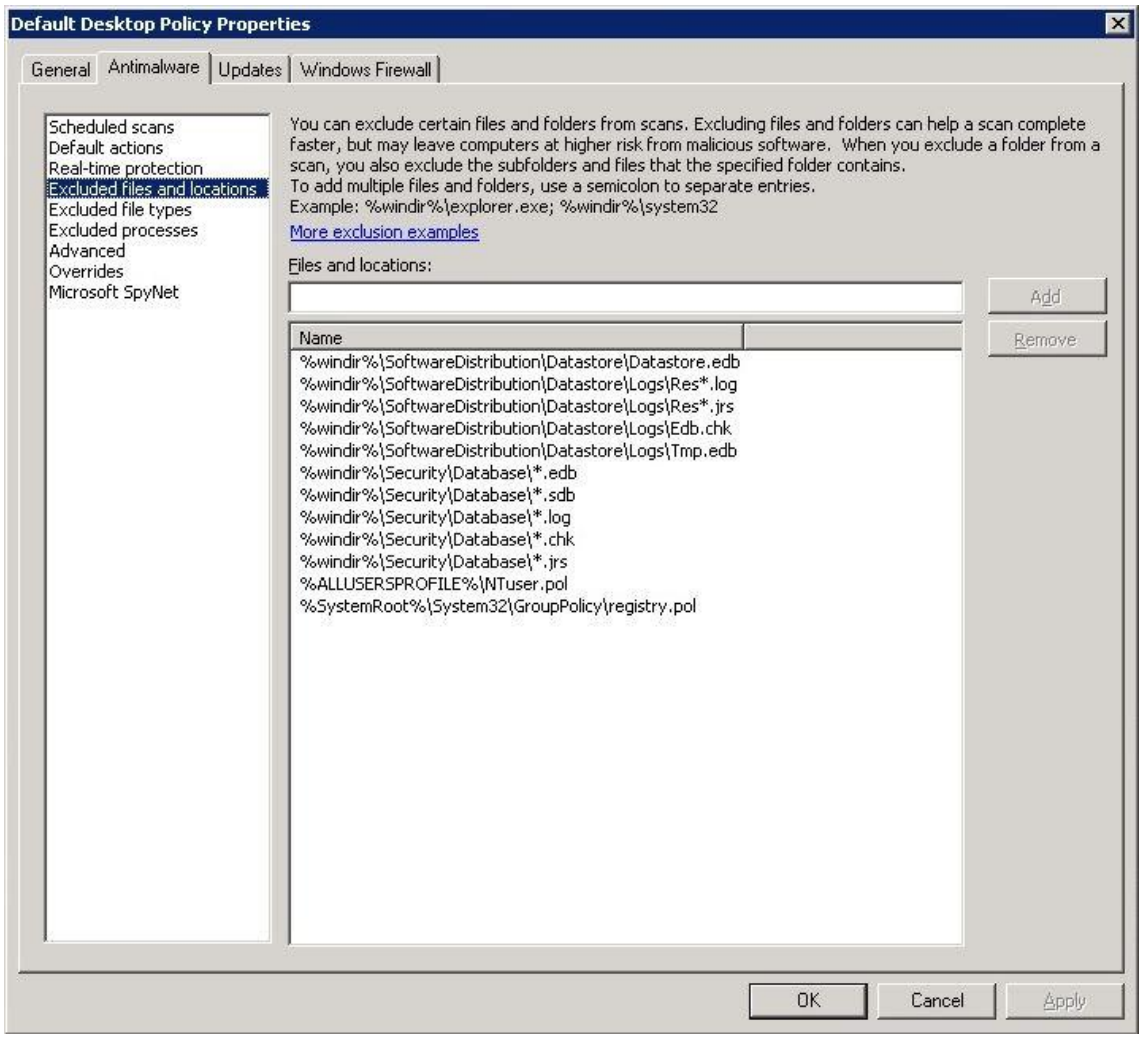
Kuva 16. Antimalware-välilehden Default actions -asetukset.

Kolmantena asetuksissa on Real-time protection -asetukset (kuva 17), jossa määritellään FEP 2010:n reaaliaikainen suojaus. Reaaliaikainen suojaus on mahdollista laittaa pois päältä, mikä tulisi jättää päälle. Tosin suositeltavaa on valita kaikki esillä olevat tietoturvatoimenpiteet, joihin kuuluvat ladattujen tiedostojen skannaus, käytösmonitorointi ja suojaus tietoverkkopohjaisia hyökkäyksiä vastaan. Lopuksi voi antaa käyttäjälle oikeudet asetuksien muokkaamiseen, mikä ei ole suositeltavaa.



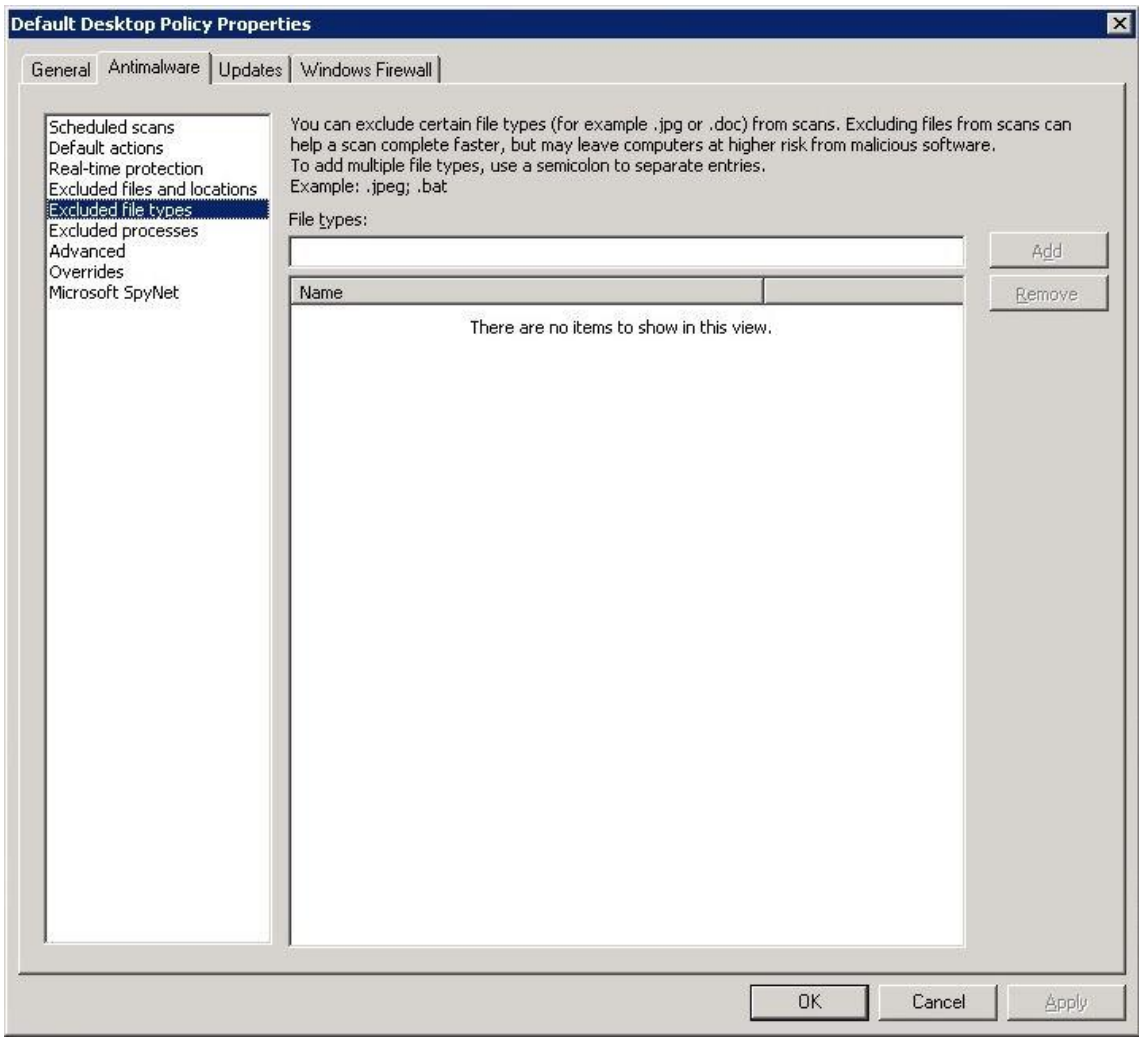
Kuva 17. Antimalware-välilehden Real-time protection -asetukset.

Excluded files and locations -asetuksissa (kuva 18) määritellään tiedostot ja sijainnit, jotka tulisi sulkea pois skannauksesta. Oletuksena ovat valittuna turvalliset tiedostot ja sijainnit, mitkä voisivat turhaan rasittaa skannausta. Voidaan lisätä ja poistaa tarpeen vaatiessa omia tiedostoja ja sijainteja, jotka ovat turvallisia. Tosin tietoturvariski kasvaa sen mukaan, mitä enemmän tiedostoja suljetaan pois skannauksesta. Tämän vuoksi pitäisi olla hyvin tarkkana pois suljettavien tiedostojen turvallisuudesta.



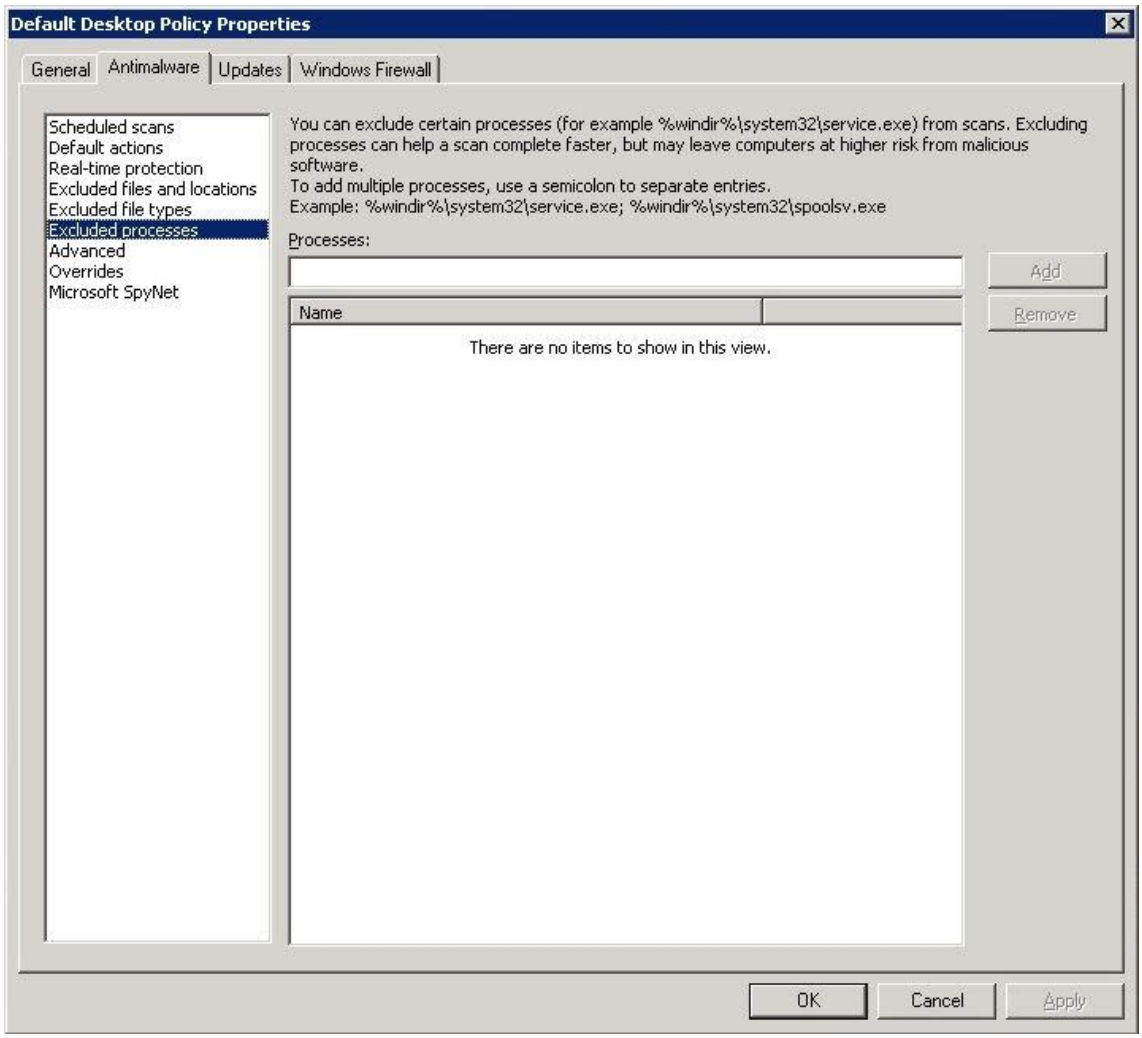
Kuva 18. Antimalware-välilehden Excluded files and locations -asetukset.

Excluded file types -asetukset (kuva 19) vastaavat edellisiä asetuksia, mutta tässä valitaan pois luettavia tiedostotyyppejä. Poistamalla tiedostotyypit, jotka tiedetään turvallisiksi, on mahdollista nopeuttaa skannausta. Tosin on suositeltavaa skannata kaikki tiedostotyypit maksimaalisen tietoturvan takia.



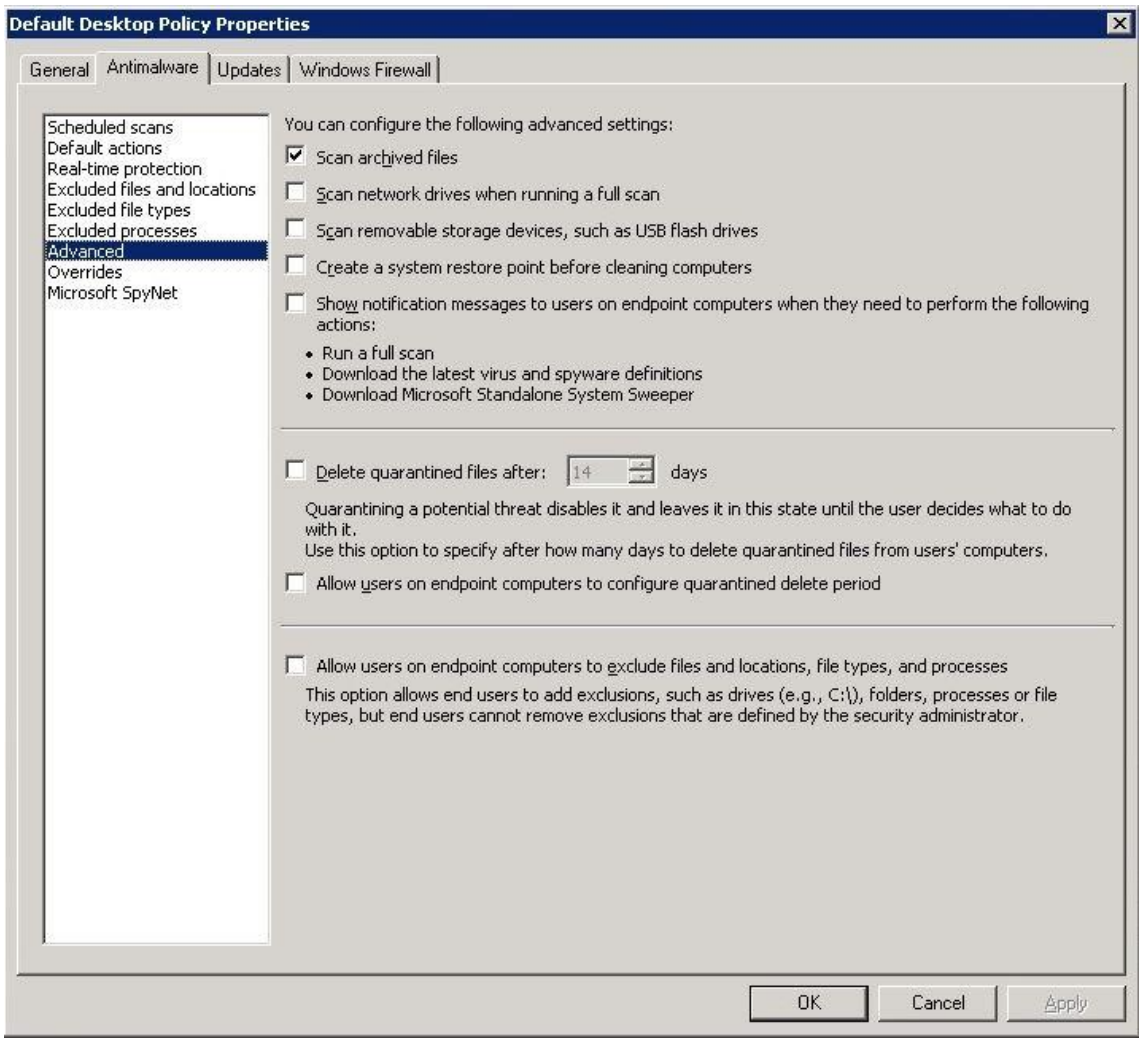
Kuva 19. Antimalware-välilehden Excluded file types -asetukset.

Seuraavana oleva Excluded processes -asetukset (kuva 20) kuuluvat samaan kategoriaan edellisten kanssa. Tässä vaiheessa on mahdollista valita prosesseja, joita ei tarkisteta skannauksessa. Suositeltavaa olisi skannata kaikki prosessit, mutta määrätyt turvalliset ohjelmaprosessit pitäisi voida lukea pois skannauksista ilman suurta tietoturvariskiä.



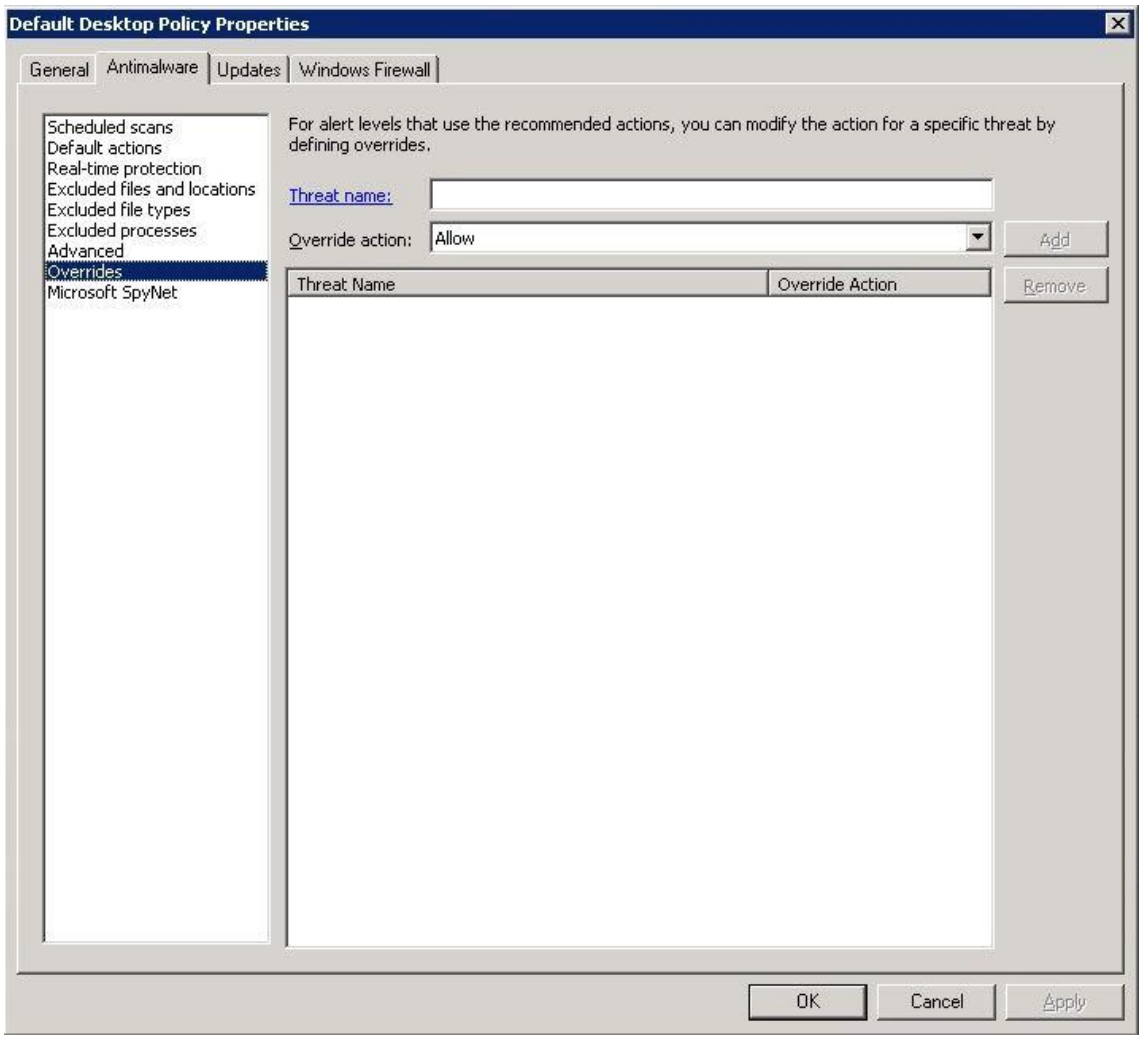
Kuva 20. Antimalware-välilehden Excluded processes -asetukset.

Advanced-asetuksissa (kuva 21) on tietoturvaan liittyviä lisäasetuksia. Asetuksissa voi määritellä muun muassa, skannataanko arkistoidut tiedostot, verkkolevyt tai mahdolliset USB-massamuistilaitteet. Voidaan myös tehdä järjestelmän palautuspiste ennen tietokoneen puhdistamista ja hallinnoida karanteenissa pidettävien mahdollisesti saastuneiden tiedostojen pitoaikaa. Käyttäjille voi antaa oikeudet lukea pois tiedostoja, sijainteja ja prosesseja skannauksista, mutta tämä ei ole suositeltavaa.



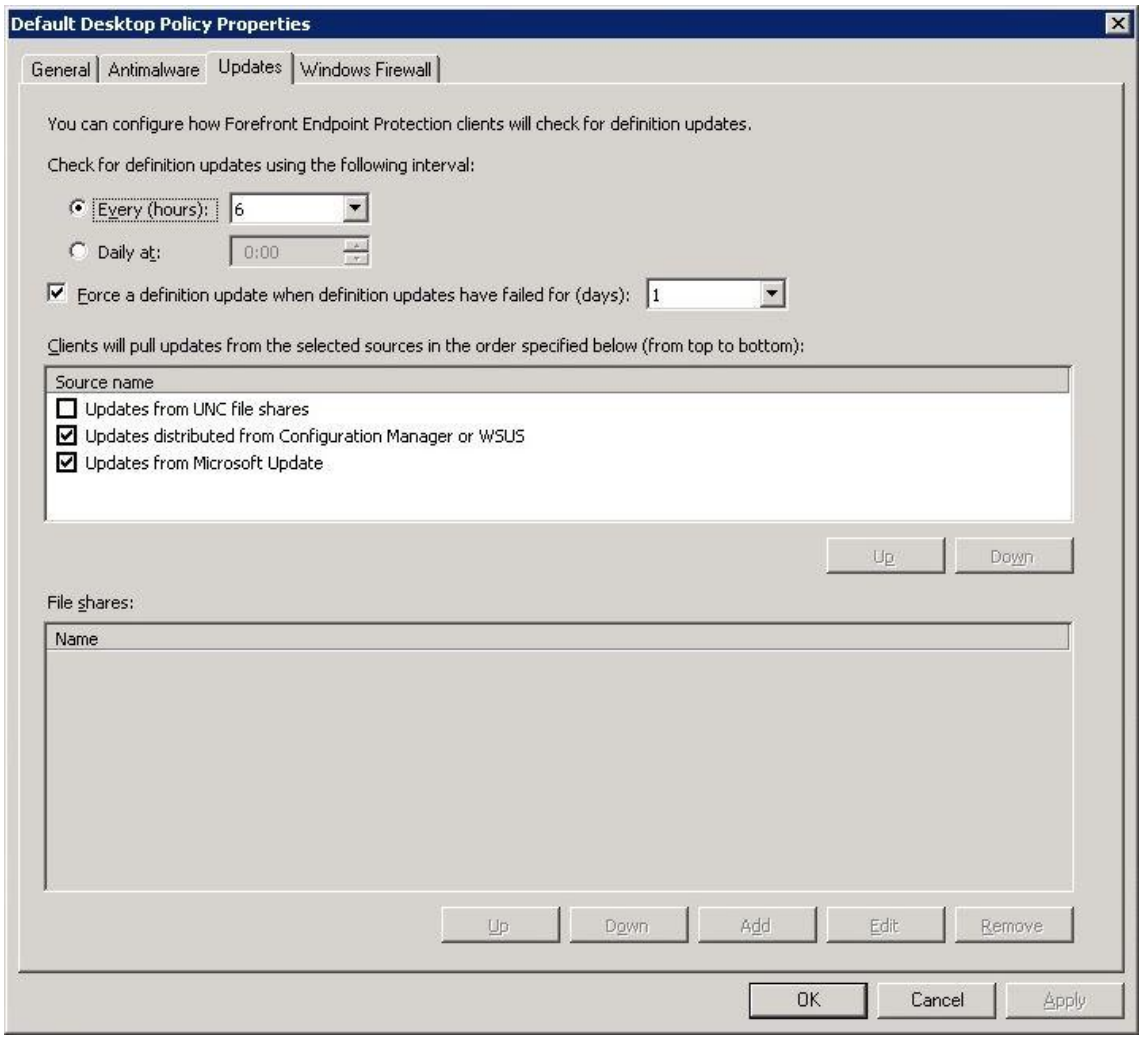
Kuva 21. Antimalware-välilehden Advanced-asetukset.

Overrides-asetuksissa (kuva 22) voi hienosäätää toimenpiteitä eri tason tietoturvauhille, joille on valittuna Recommended actions -kohta. Tämä mahdollistaa omien tietoturvasääntöjen luomisen, jos esimerkiksi erikseen määritelty haittaohjelma tunkeutuu tietoverkkoon. Säännöillä voi myös sallia haittaohjelmaksi luokiteltujen turvallisten ohjelmien toiminnan. Tietoturvaohjelmistot saattavat esimerkiksi luokitella itse tehtyjä ohjelmistoja tietoturvauhiksi.



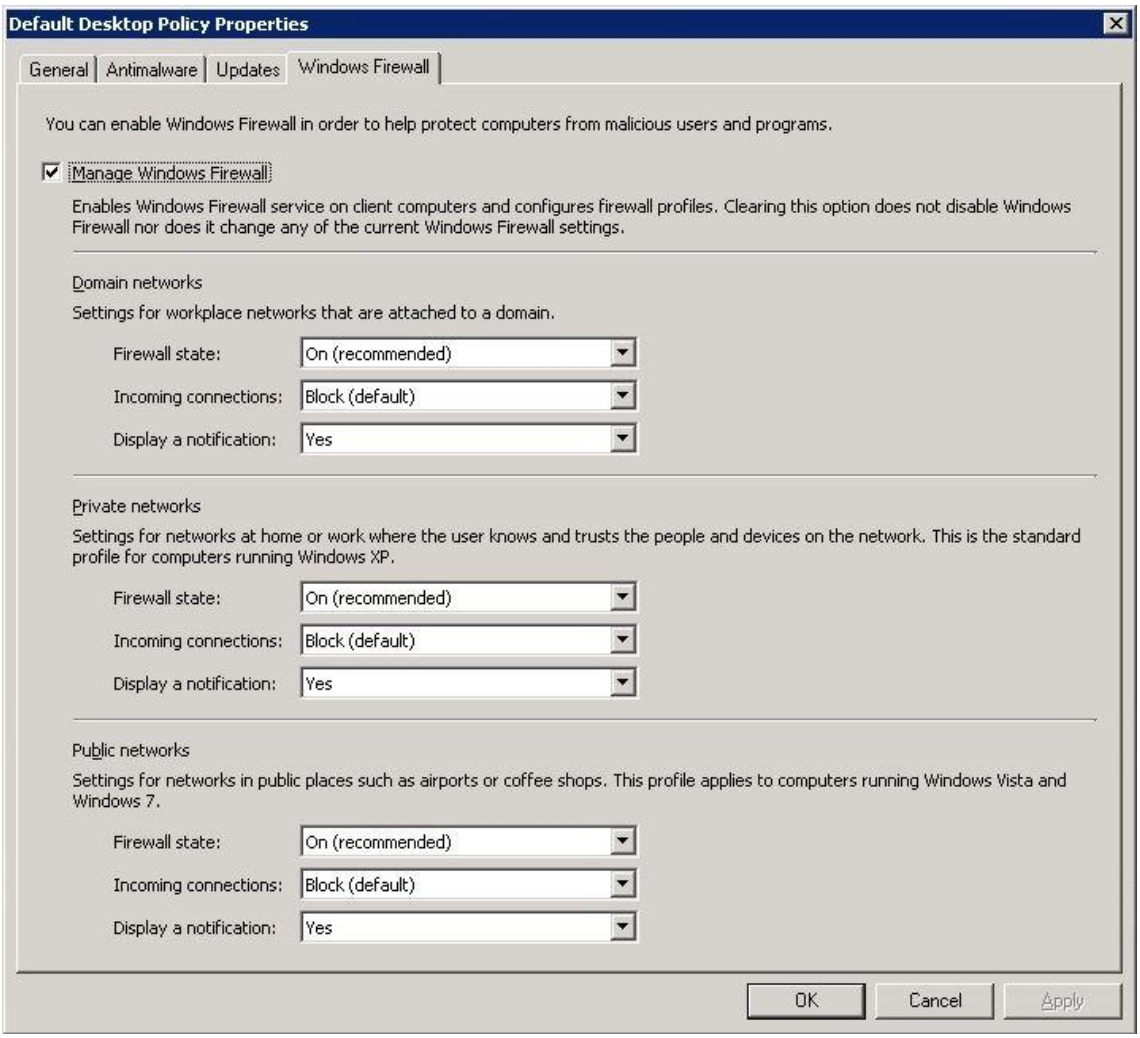
Kuva 22. Antimalware-välilehden Overrides-asetukset.

Seuraavana on Updates-välilehti (kuva 23), jossa ovat asetukset koskien virustietokannan päivittämistä. Päivityksien tarkistuksen voi suorittaa joko asetettujen tuntien välein tai päivittäin määrättynä kellonaikana. Päivitykset voi myös pakottaa, jos päivittäminen on epäonnistunut määriteltyjen päivien ajan. Asetuksissa valitaan myös päivityksien latauslähteet. Päivitykset voidaan ladata UNC-tiedostojaolla, Microsoft Configuration Managerin kautta tai käyttämällä WSUS:ta. UNC, eli Universal Naming Convention, on nimeämisformaatti palvelimien ja muiden verkon laitteiden sijaintien löytämiselle. (10.) WSUS, eli Windows Server Update Services, on päivityksien jakamispalvelu Windows-verkkoympäristöön. (11.) Päivitykset kannattaa myös asettaa latautumaan Microsoft Windows Update -palvelun kautta, jolloin myös toimialueen ulkopuoliset asiakastietokoneet voivat saada uusimmat päivitykset.



Kuva 23. Updates-välilehden asetukset.

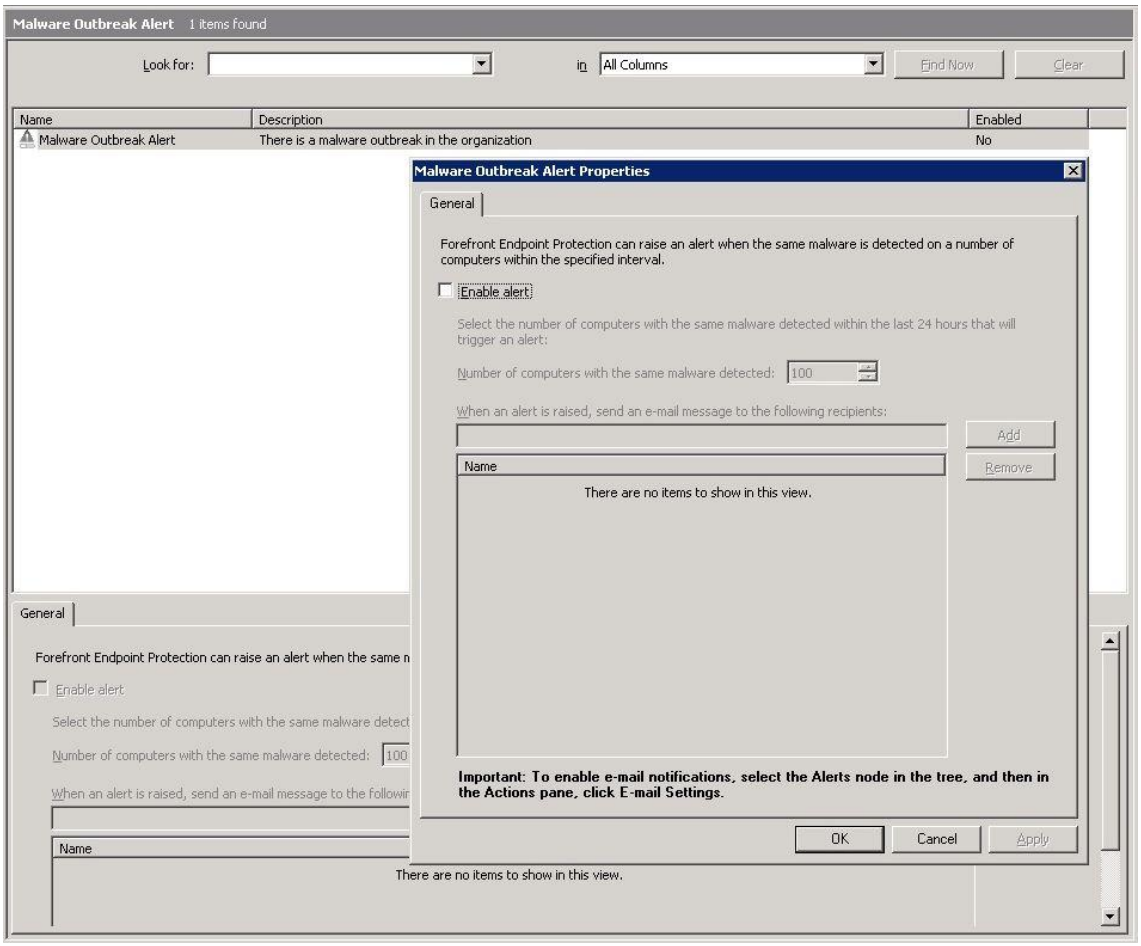
Viimeisenä asetuksissa on Windows Firewall -välilehti (kuva 24), jossa ovat asetukset koskien FEP 2010 käyttämää Windows-palomuuria. Asetuksissa voi laittaa palomuurin päälle tai pois päältä, sekä sallitaanko sisään tulevat yhteydet. Asetukset ovat erikseen toimialueelle, sen ulkopuolisille turvallisille verkoille ja julkisille verkoille. Tämä mahdollistaa esimerkiksi työkannettavan palomuuri asetuksien säätämisen sen mukaan, missä kyseinen tietokone sijaitsee. Voidaan myös asettaa ilmoituksen näkyviin käyttäjille tulevista yhteysyrityksistä.



Kuva 24. Windows Firewall -välilehden asetukset.

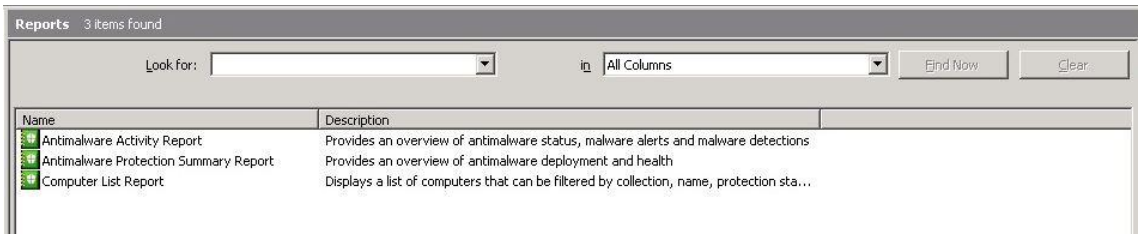
5.2 Hälytykset ja raportit

FEP 2010 sisältää mahdollisuuden suorittaa hälytyksiä tietomurroista sähköpostilla sekä kattavat raportointiominaisuudet. Menemällä Forefront Endpoint Protection -> Alerts -> Malware outbreak ja siellä Properties-asetuksiin (kuva 25). Hälytys asetuksissa on mahdollista lähettää huomautussähköposti valituille osoitteille tietomurron sattuessa. Jotta järjestelmä ei lähettäisi hälytyksiä jokaisesta tietoturvariskistä, voi asetuksille antaa määrätyn lukumäärän saastuneista koneista. Tämä tarkoittaa, ettei hälytystä lähetetä kunnes esimerkiksi 100 tietokonetta ovat saastuneet. Luku tulisi muuttaa tietenkin tietoverkossa olevien laitemäärien mukaan.



Kuva 25. FEP 2010:n hälytysvalinta mahdollisen tietomurron sattuessa.

FEP 2010 tarjoaa raportointityökalut useaan eri tarpeeseen (kuva 26). Raportit on mahdollista luoda koskien yleistä tietoturva tilannetta FEP 2010 turvatuissa laitteissa. Tämä esimerkiksi raportoi hälytykset ja mahdolliset haittaohjelmien havainnot. Raportin voi myös luoda koskien FEP 2010:n päivittymistä verkkoon. Tästä muun muassa näkee, mitkä laitteet ovat saaneet uusimmat päivitykset tai ovat mahdollisesti pois päältä. Jos esimerkiksi ohjelman jakelussa esiintyy ongelmia, se voidaan raportoida helposti tarpeen vaatiessa. Kaikkien FEP 2010:n kokoelmassa olevien laitteiden listaus kokoelman, nimen ja suojaustilan mukaan on mahdollista.



Kuva 26. FEP 2010:n raportointityökalut.

Tässä vaiheessa FEP 2010:n pitäisi olla periaatteessa toimintavalmis. Kun FEP 2010 on asennettu ja konfiguroitu toimimaan käsiasennetussa testiverkossa, tulee sen käyttöä testata. Seuraavassa luvussa verrataan FEP 2010:n ja F-Securen toimintaa keskenään, sekä testataan FEP 2010 -tietoturvaa.

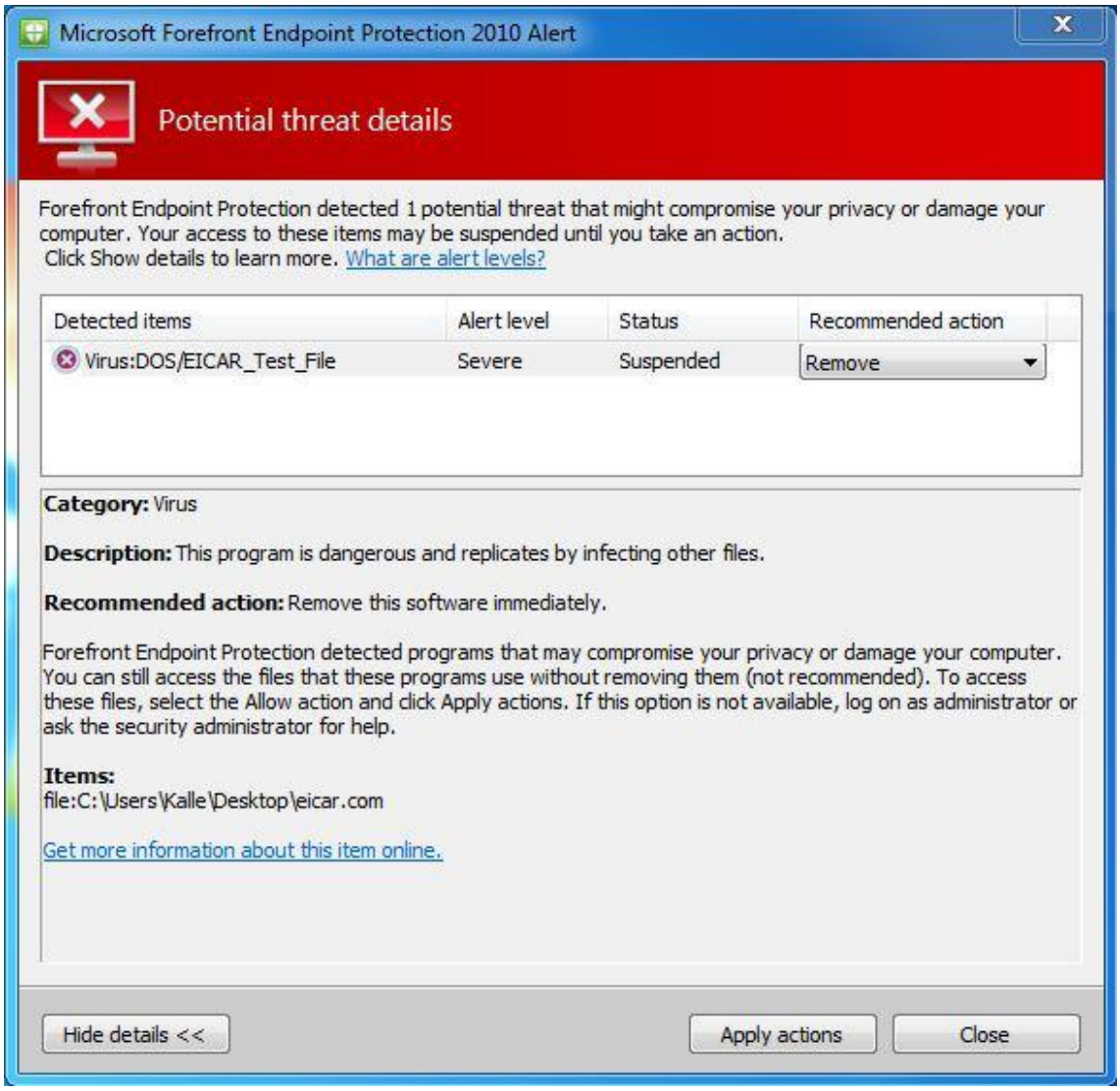
6 Testaus

On hyvin tärkeää testata uutta järjestelmää sen jälkeen, kun testiryhmä on asennettu käyttöön. Vasta uuden järjestelmän testauksen jälkeen kannattaa testiryhmä laajentaa suuremmille määrille tietokoneita. Projektissa oli tarkoitus verrata FEP 2010:n nopeutta nykyiseen F-Securen tietoturvajärjestelmään sekä testata virustorjunnan tehokkuutta. Täten on helpompi verrata nykyisen järjestelmän vaihtamisen kannattavuutta Microsoftin tietoturvaratkaisuun.

6.1 Virustesti

Virustestissä oli tarkoitus katsoa, kykeneekö FEP 2010 havaitsemaan esimerkiksi virusohjelman lataamisen selaimella ja kuinka järjestelmä ilmoittaa asiasta hallintapaneeliin SCCM-palvelimelle. Testissä käytettiin eicar-testitiedostoa. Kyseessä on sertifioitu ja harmiton virustiedosto, jolla on mahdollista testata tietoturvaohjelmistojen perustoimintaa. Jos ohjelmisto ei havaitse eicar-tiedostoa, niin virustorjunnassa on puutteita. Eicar-testiviruksen saa ladattua osoitteesta http://www.eicar.org/.

Eicar-testitiedosto ladattiin .com- ja .txt-päätteisinä sekä zip-tiedostona. Lisätestinä eicar-testivirus yritettiin myös kirjoittaa ja tallentaa testikoneelle. Ohje eicar-testiviruksen tekemiseen löytyy liitteestä 1. FEP 2010 onnistui havaitsemaan kaikki latausyritykset onnistuneesti (kuva 27) sekä esti virustiedoston tallennuksen testikoneelle (kuva 28).



Kuva 27. Kuva FEP 2010:n näyttämästä ilmoitusviestistä mahdollisen viruksen löytämisestä.

Kuva 28. Kuva FEP 2010:n ilmoituksesta, kun eicar.com yritettiin tallentaa tietokoneelle.

FEP 2010:n ilmoitus on informatiivinen ja hallintapaneeliin SCCM-palvelimella tuli näkyviin mahdollinen tartuntatapaus. Tämä helpottaa järjestelmänylläpitäjän työtä löytämään ja eristämään mahdolliset tartuntatilanteet. Koska FEP 2010 havaitsi eicar-testiviruksen, niin voi todeta järjestelmän virustorjunnan olevan toiminnassa. FEP 2010 myös poisti testiviruksen onnistuneesti tietokoneelta.

6.2 Nopeustesti

Nopeustestissä testattiin F-Securen ja FEP 2010:n välisiä nopeuseroja testikoneella. Testausmenetelminä käytettiin käsin sekuntikellolla mitattua aikaa kirjautumisessa tietokoneelle, sekä PCMark05-testausohjelmiston tuloksia. PCMark05-ohjelmiston voi ladata osoitteesta http://www.futuremark.com/products/pcmark05/. Tuloksia verrattiin keskenään ja sen perusteella todettiin, mikä ohjelmistoista on nopeampi järjestelmälle. Testikoneessa oli Intel Core 2 Duo E7300 2,66 GHz suoritin, 4 Gt keskusmuistia ja Windows 7 professional -käyttöjärjestelmä.

Järjestelmän käynnistystestissä mitattiin aikaa, joka kului kirjautumisesta sisään ja käyttöjärjestelmän työpöydän valmiustilan välillä. Koska testi suoritettiin käsimittauksella silmämääräisesti, mahdollinen virhemarginaali tulee ottaa tuloksissa huomioon. Testituloksista voi huomata, että FEP 2010 nopeutti tietokoneen kirjautumista keskimäärin kuudella sekunnilla (taulukko 5).

Taulukko 5. Testikoneen sisäänkirjautumistestin tulokset.

	F-Secure	**FEP 2010**	**Nopeusero**
1. käynnistys	27 s	30 s	-3 s
2. käynnistys	34 s	20 s	+14 s
3. käynnistys	24 s	15 s	+9 s
Keskiarvo	28 s	22 s	+6 s

Seuraavaksi testattiin, onko suuren tiedoston kopioimisessa nopeuseroja. Tämä johtuu siitä, että joidenkin tietoturvaohjelmistojen reaaliaikainen skannaaminen saattaa hidastaa kyseisiä toimenpiteitä. Testikoneella kopioitiin 2,07 Gt kokoinen iso-tiedosto kansi-

osta toiseen ja mitattiin aika sekuntikellolla. F-Securen käytössä ajaksi saatiin 1 min 52 s ja FEP 2010:n kanssa 1 min 55 s. Tuloksista voi todeta, ettei tiedoston kopioimisessa ollut nopeuseroa.

Lopuksi testikoneella ajettiin Futuremarkin PCMark05-suorituskyvynmittausohjelma, joka testaa tietokoneen kykyä useissa eri toiminnoissa. Ohjelma esimerkiksi testaa käynnistymistä, moniajoa ja lukunopeuksia. PCMark05 antaa testin suoritettua pistetuloksen, joka on vertailukelpoinen muiden tuloksien kanssa. Saatuja tuloksia vertaamalla voidaan todeta, että nopeuserot ovat hyvin pienet kahden tietoturvaohjelmiston välillä (taulukko 6).

Taulukko 6. PCMark05:n pistetulokset testikoneella.

	F-Secure	**FEP 2010**	**Nopeusero**
PCMark05 pisteet	4446	4421	0,56 %

Saatujen tuloksien perusteella voidaan todeta, että ainoa mahdollinen nopeusetu F-Securen tietoturvaratkaisuun nähden olisi mahdollisesti nopeampi tietokoneen käynnistyminen. Koska nopeuserot osoittautuivat niin pieniksi, eivät ne vaikuta tietoturvajärjestelmän vaihtamiseen. Vaikuttavia tekijöitä ovat täten yksinkertaisuus, tietoturvan tehokkuus ja käyttäjäystävällisyys.

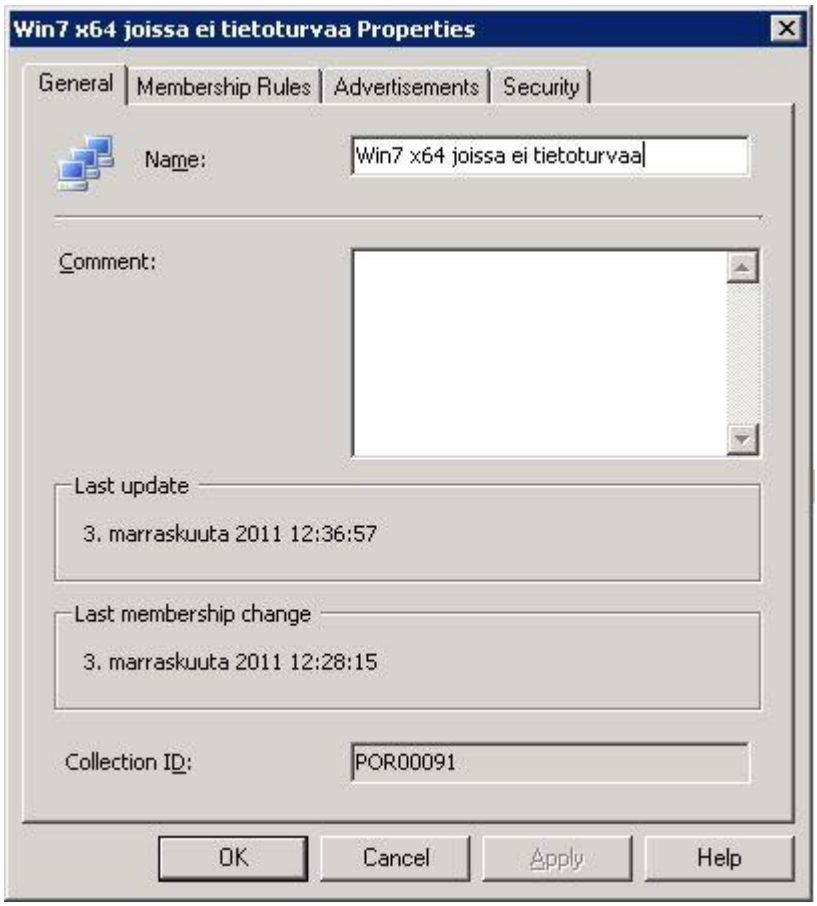
7 Ohjelmiston levittäminen Configuration Managerilla

FEP 2010 tietoturvan toimivuuden ja nopeuden testaamisen jälkeen oli aika keksiä järkevä ratkaisu ohjelmiston levittämiselle suuremmalle määrälle tietokoneita. Tämän mahdollistaa Microsoftin Configuration Managerin ohjelmien mainostustoiminnot, jonka avulla on mahdollista jakaa esimerkiksi FEP 2010 määrättyihin tietokoneisiin. Tässä luvussa käydään läpi työvaiheet ja kriteerit, joiden perusteella FEP 2010 voidaan jakaa tietoverkkoon.

7.1 Kokoelmat ja kriteerit

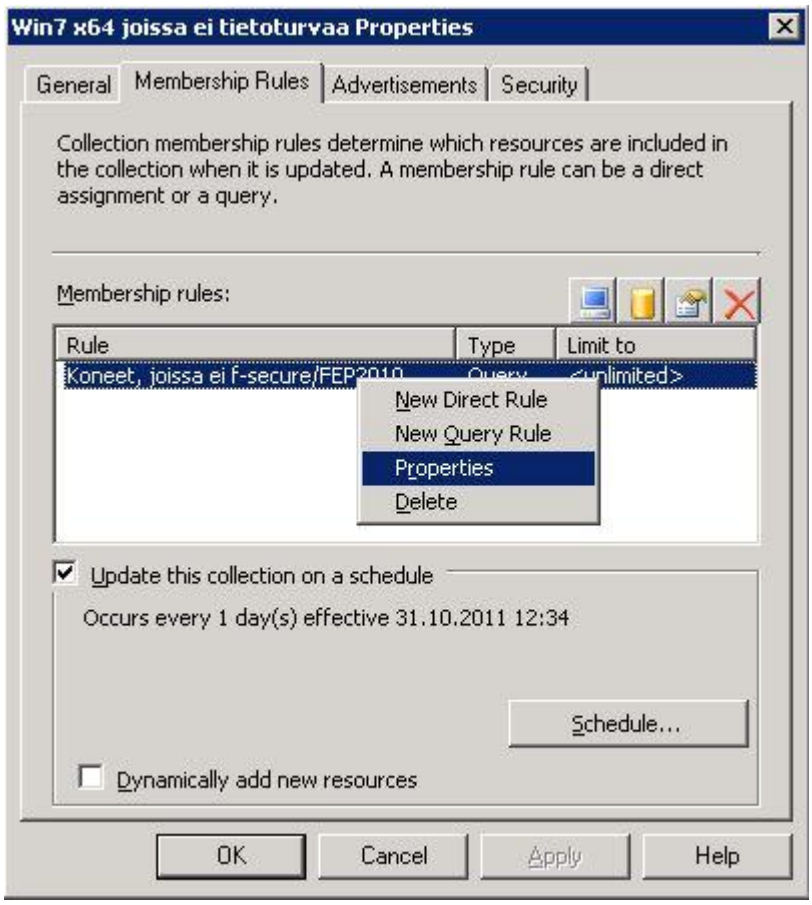
Ennen FEP 2010:n levitystä tuli miettiä, millaisilla kriteereillä ohjelmistoa tulisi levittää toimialueen tietokoneisiin. Kokoelman pitäisi huomioida tietokoneiden käyttöliittymän ja tietoturvaohjelmistojen tilan. FEP 2010 saisi asentua vain tietokoneille, joissa on 64-bittinen Windows 7 asennettuna, eikä tietokoneilla saisi olla asennettuna F-Securen tietoturvaohjelmistoa samaan aikaan. Uuden kokoelman on mahdollista tehdä menemällä Site database -> Computer management -> Collections. Oikealla hiiren painikkeella aukeavasta kontekstivalikosta tulee valita new collection -kohta.

Projektissa tehtiin kokoelma tietokoneille, joihin oli valmiiksi asennettuna F-Securen tietoturvaohjelmisto. Tämän avulla oli mahdollista määritellä uusi kokoelma, joka sisältää vain tietokoneet, joissa ei ole tietoturvaa asennettuna. Ideana oli automatisoida FEP 2010 -ohjelmiston asentaminen tietokoneille sitä mukaan, kun F-Secure poistetaan. Sitä varten tuli tehdä uusi kokoelma. Tehdyn kokoelman asetuksien ”General” välilehdeltä (kuva 29) tulee ensiksi valita nimi kokoelmalle. Samalta sivulta näkee myös kokoelman ID-arvon, johon viitataan esimerkiksi kriteerejä tehtäessä.



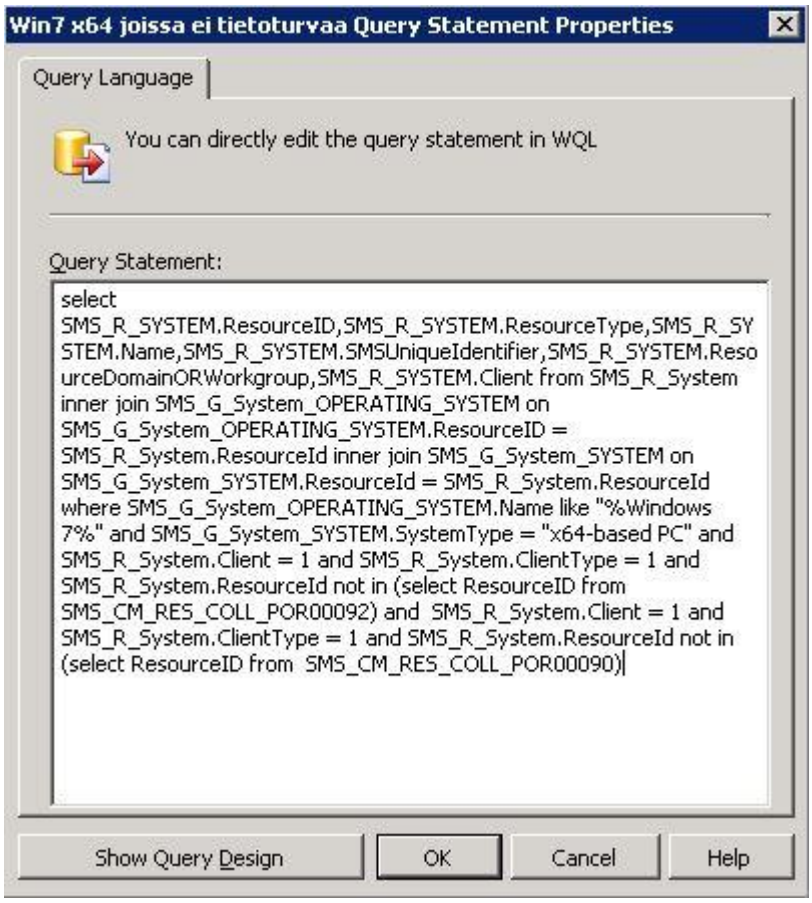
Kuva 29. Kokoelman asetuksien General-välilehti.

Membership Rules -välilehti (kuva 30) on asetuksista tärkein. Siinä määritellään muun muassa kriteerit, joiden perusteella kokoelmaan valitaan laitteet. Sääntöjä voi tehdä lisää tai muokata. Projektissa muokattiin olemassa olevaa sääntöä, joka luotiin kokoelmaa tehtäessä. Sääntöä voi muokata valitsemalla kontekstivalikosta Properties-kohta.



Kuva 30. Kokoelman asetuksien Membership Rules -välilehti.

Kriteerejä on mahdollista lisätä kahdella tapaa. Kriteerit voidaan valita graafisesti valikoiden kautta tai kirjoittamalla kriteerit WQL-kielellä. Projektissa kriteerit valittiin graafisen käyttöliittymän avulla, jonka saa myös näkyviin WQL-kielelle (kuva 31). WQL-kieli on SQL-kielen johdannainen pienillä muutoksilla, jotta se sopisi WMI ympäristöön. (12.) Tietokoneessa tuli olla Windows 7 -käyttöjärjestelmä, järjestelmän tuli olla 64-bittinen ja tietokone ei saa kuulua F-Secure-kokoelmaan, joka luotiin aiemmin. Näillä kriteereillä tehtyyn kokoelmaan sisältyisi vain ne tietokoneet, joihin FEP 2010 olisi turvallista asentaa. Aiemmin mainittua kokoelman ID-arvoa tarvittiin F-Secure-kokoelman määrittämisessä.

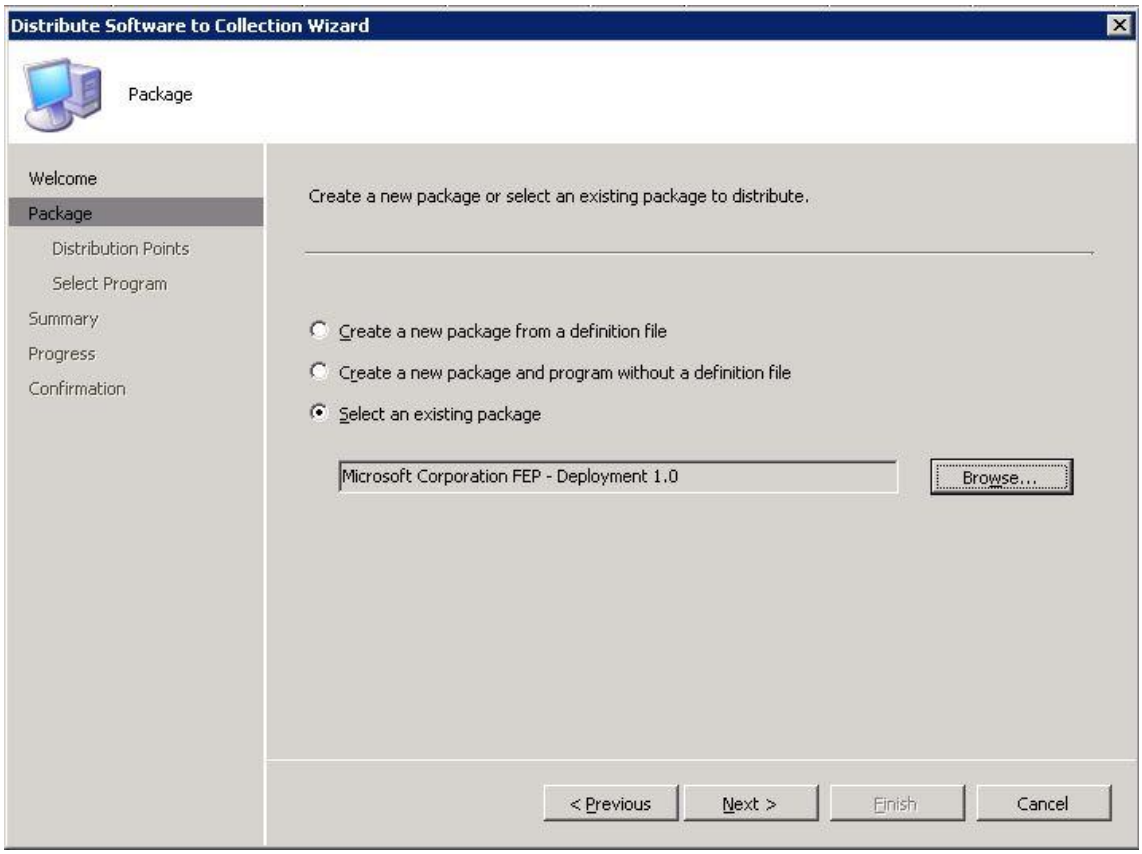


Kuva 31. Kokoelman kriteerit WQL-kielellä.

Kun kokoelman säännöt ja kriteerit oli asetettu oikein, voitiin siirtyä seuraavaan työvaiheeseen. Kriteerit tulisi testata ja tarkistaa huolella ennen ohjelmiston jakamista kokoelman laitteille. Esimerkiksi päällekkäiset tietoturvaohjelmistot voivat aiheuttaa tietoliikenteen toimimattomuuden tai muuta epävakaisuutta.

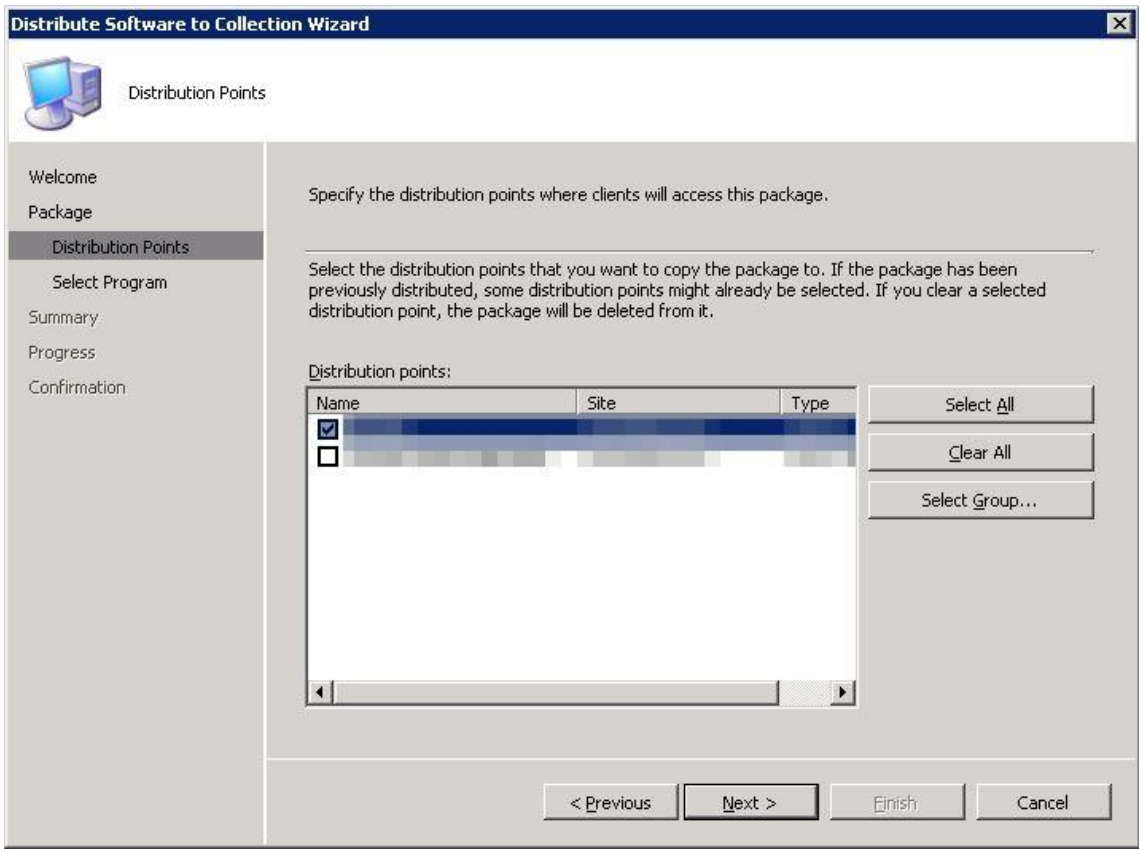
7.2 FEP 2010:n jakaminen

Ohjelmiston jakaminen suoritettiin Configuration managerin mainostustyökalulla. Ensiksi valitaan kokoelma, jonka tietokoneille halutaan asentaa FEP 2010 -ohjelmisto. Tämän jälkeen hiiren oikean näppäimen kontekstivalikosta valitaan Distribute -> Software. Eteen tulevasta asennusvelhon Package-vaiheessa valitaan ohjelmistopaketti levitykseen. Projektissa käytetty FEP 2010 levityspaketti löytyy, kun valitaan Select an exciting package -kohta ja browse-napista hakemalla Microsoft Corpration FEP – Deployment 1.0 -niminen paketti (kuva 32).



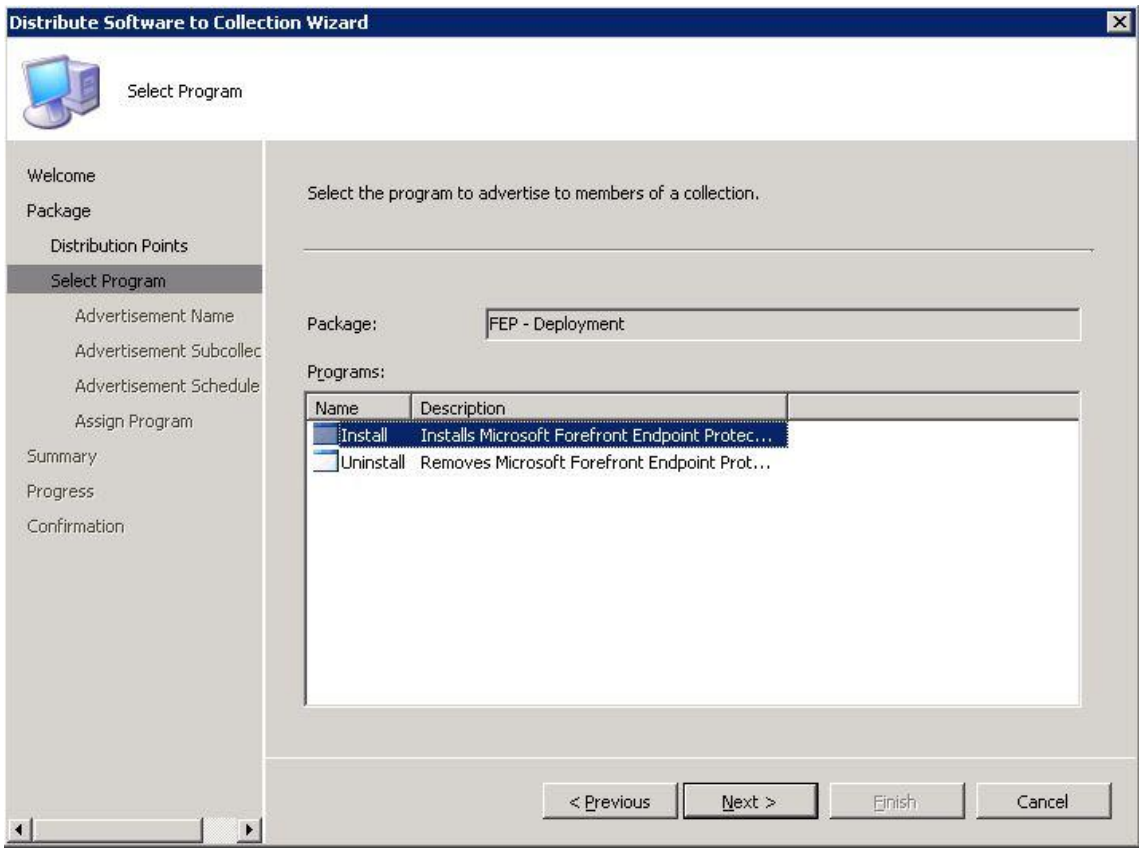
Kuva 32. Asennusvelho kysyy, mikä ohjelmistopaketti levitetään.

Seuraavaksi tulee valita jakopisteet, joiden kautta pakettia mainostetaan (kuva 33). Jakopisteet ovat sijainteja, joihin mainostettava asennuspaketti tallennetaan. Tällöin tietokoneet, jotka kuuluvat mainostuksen piiriin, voivat ottaa yhteyttä jakopisteeseen, jonka kautta asennus suoritetaan.



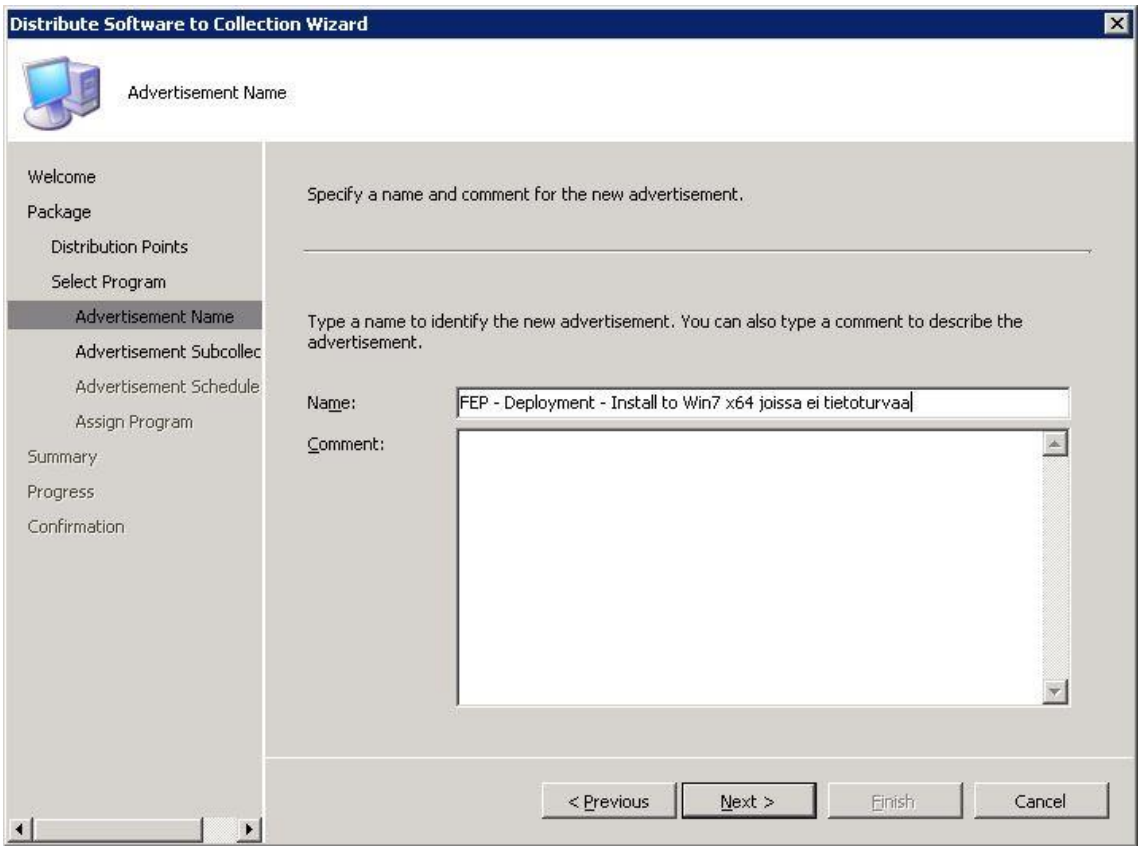
Kuva 33. Asennusvelho pyytää valitsemaan jakopisteet.

Jakopisteen valinnan jälkeen kysytään, mitä ohjelmaa jaetaan (kuva 34). FEP 2010:n tapauksessa tarjolla on asennus- ja poisto-ohjelmat. Tässä tapauksessa siis valitaan asennusohjelma Install-valinta ja tarpeen vaatiessa myöhemmin FEP 2010:n poistaminen on helppoa valitsemalla Uninstall-valinta.



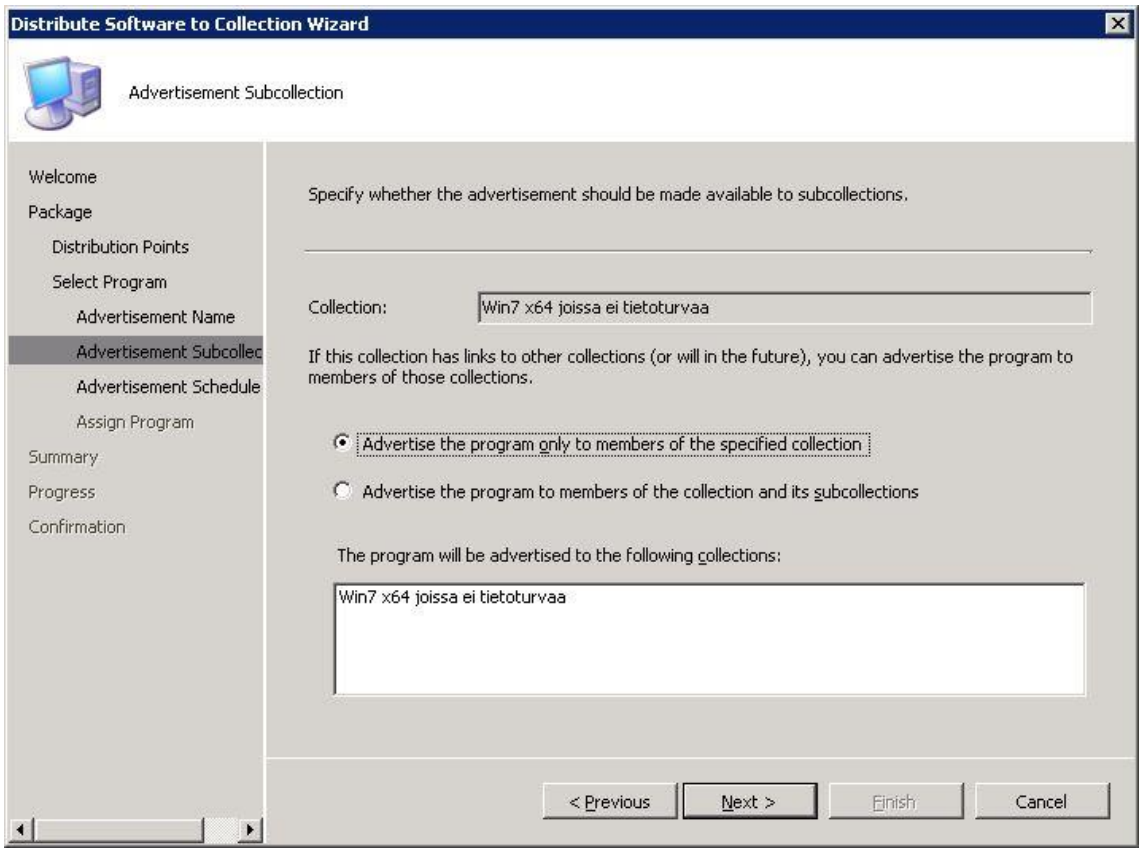
Kuva 34. Asennusvelhossa valitaan asennustoimenpide.

Seuraavana on ohjelman mainostukseen liittyvät asetukset. Näissä ensimmäisenä tulee antaa nimi uudelle mainostukselle (kuva 35). Nimen olisi hyvä kuvata tarkasti, mitä mainostus käsittelee, jolloin sen löytäminen ja hallinta on helppoa myöhemmin. Lisäkommenttien kirjoittaminen voi olla myös suotavaa riippuen tilanteesta.



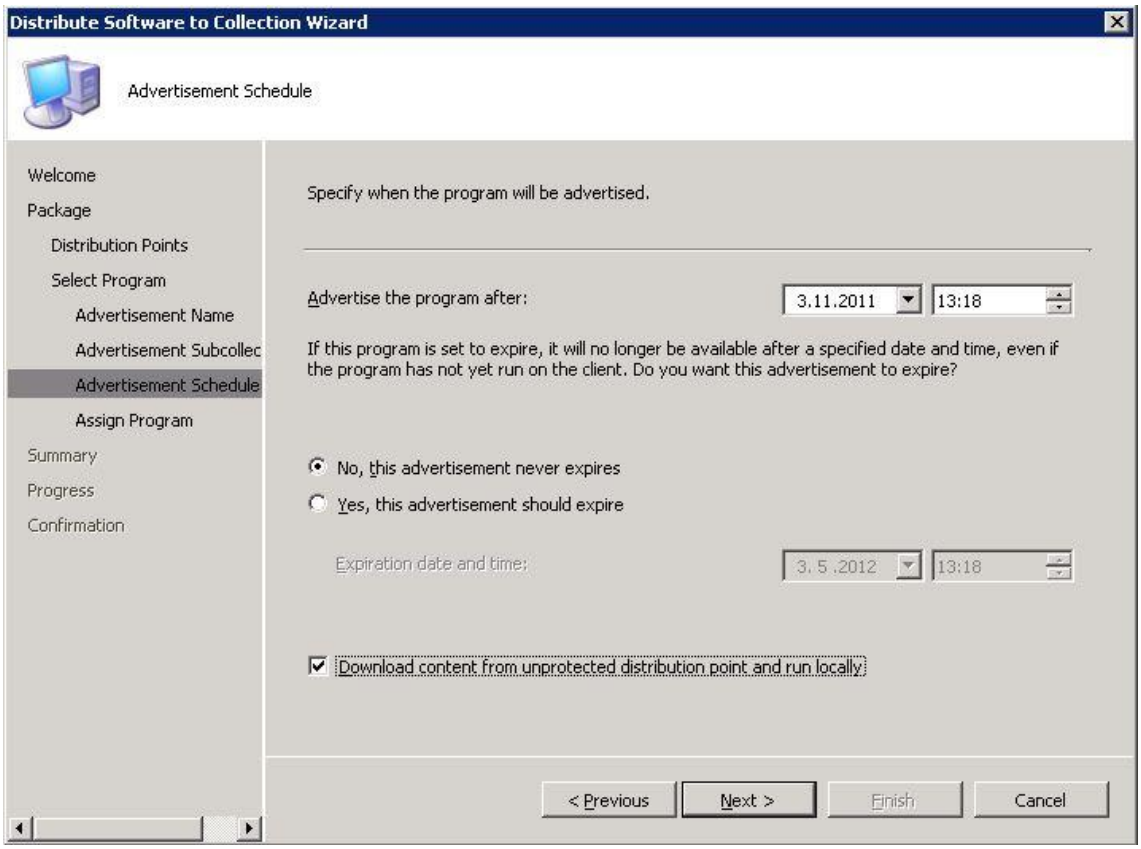
Kuva 35. Mainostukselle valitaan nimi.

Nimen valinnan ja kommentoinnin jälkeen tulee valita, mihin kokoelmaan mainostus jaetaan (kuva 36). Kokoelma, joka valittiin aiemmin jo heti asennuksen alussa, pitäisi olla oletuksena valittuna. Tässä tapauksessa kyseessä on kokoelma, joka sisältää tietokoneet, joissa ei ole F-Securen tietoturvaa asennettuna. Jos kyseisellä kokoelmalla olisi muita jäseniä ja alikokoelmia, olisi mahdollista valita mainostus myös näille laitteille. Projektissa tämä ei ollut tarpeen, koska kyseessä on yksinkertainen yhtä asiaa käsittelevä kokoelma.



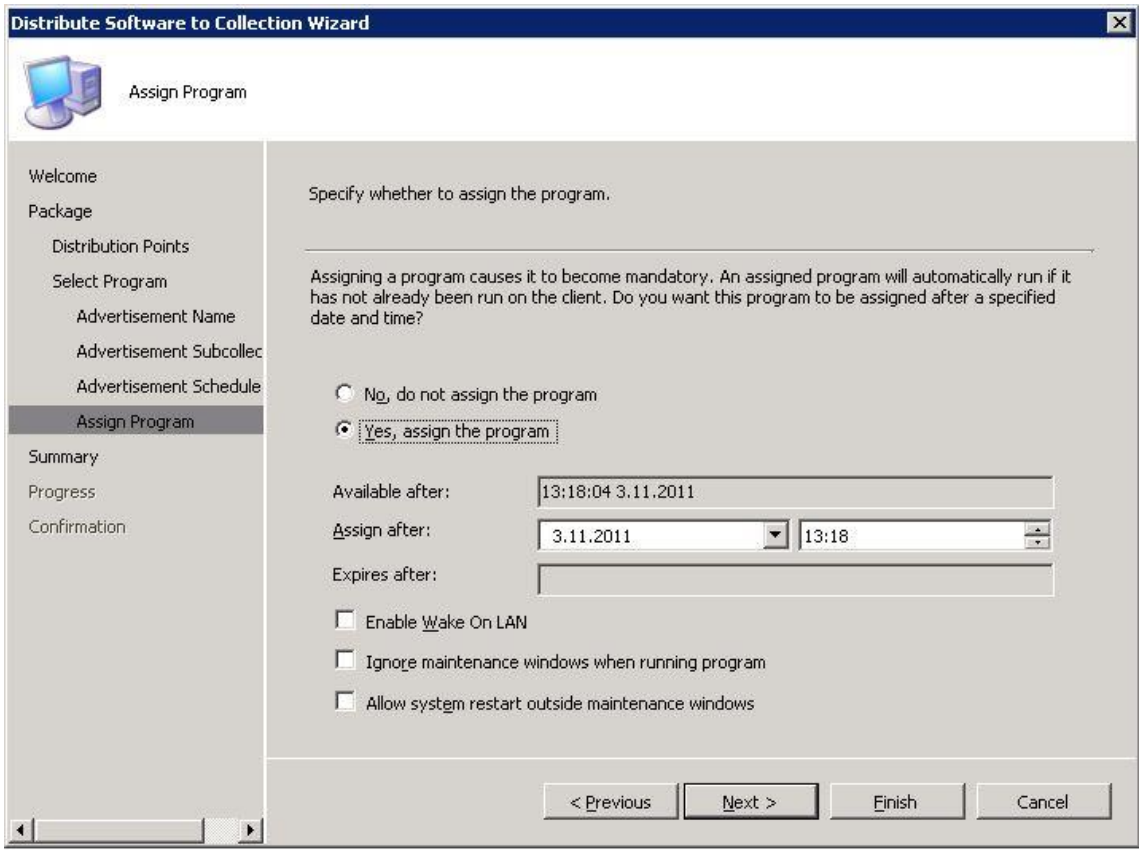
Kuva 36. Mainostusasetukset ohjelman jakamisesta myös mahdollisiin alikokoelmiin.

Mainostuksen ajoitus on seuraavana asetuksissa (kuva 37). Aluksi tulee määrittää, milloin ohjelman mainostaminen aloitetaan. Jos ei esteitä ole, esimerkiksi laitteiden päivitys tai muu vastaava, voi mainostuksen aloittaa heti. Tarpeen vaatiessa on mahdollista myös asettaa päivämäärä, jonka jälkeen ohjelman mainostaminen lopetetaan. Projektille mainostus aloitettiin heti ja lopetuspäivämäärää ei valittu.



Kuva 37. Mainostuksen ajoituksen asettaminen

Lopuksi kysytään mainostukseen liittyvistä lisäasetuksista (kuva 38). Ensiksi tulee valita, pakotetaanko ohjelman mainostaminen. Jos valitaan Yes, assign the program -kohta, mainostettava ohjelma muuttuu pakolliseksi kaikkiin niihin laitteisiin, joissa sitä ei vielä ole. Projektissa valittiin tämä asetus ohjelman mainostukselle. Kyseiselle valinnalle voi valita tämän jälkeen aloitus- sekä lopetuspäivämäärät tarpeen mukaan. Muita lisäasetuksia ovat Wake On LAN -valinta, huoltoikkunoiden poistaminen ja järjestelmän uudelleen käynnistymisen salliminen ylläpitoikkunan ulkopuolella. Wake On LAN tarkoittaa ,että kohdetietokone voidaan herättää valvetilasta tarpeen vaatiessa. Näiden asetuksien jälkeen on enää yhteenveto, hyväksyntä ja asetuksien tarkistus jäljellä.



Kuva 38. Ohjelman lisämääritykset mainostukselle.

Kun mainostusasetukset oli tehty, täytyi odottaa FEP 2010:n asentumista valitun kokoelman tietokoneille. Tämä saattaa viedä useamman päivän riippuen tietokoneiden lukumäärästä ja niiden tiloista. Ikävä kyllä F-Secure-tietokoneisiin oli käytetty virheellistä kriteeriä ja FEP 2010 pääsi asentumaan myös osittain väärille tietokoneille. Tämä aiheutti internetyhteyksien jumittumisen kyseisissä laitteissa. Tilanne saatiin korjattua mainostamalla FEP 2010 poisto-ohjelmistoa kaikkiin Windows 7 -käyttöjärjestelmällä oleviin laitteisiin.

8 Yhteenveto ja johtopäätökset

Projektissa asennettiin FEP 2010 keskitetty tietoturvaratkaisu SCCM-palvelimelle. Palvelu saatiin toimimaan koulun verkossa ja näin ollen projektin tavoitteet saavutettiin. Tarkoituksena oli juuri testata, kuinka FEP 2010 saadaan asennettua ja toimintavalmiiksi. Järjestelmän toimintaa testattiin aluksi pienellä ryhmällä tietokoneita. Näissä

testikoneissa monitoroitiin FEP 2010 toimintaa parin viikon ajan. Ennen kuin testiryhmää laajennettiin, testattiin myös ohjelmiston nopeusvaikutus PCMark05-ohjelmistolla. Tuloksia verrattiin jo käytössä olevaan F-Securen tietoturvaratkaisuun. Nopeuseroja ei FEP 2010:n ja F-Securen välillä juuri löytynyt. Lopuksi FEP 2010 -virustentorjuntaa testattiin standardisoidulla Eicar-testiviruksella. FEP 2010 tunnisti kaikki virustestit.

Seuraavaksi oli tarkoitus levittää FEP 2010 suuremmalle määrälle tietokoneita ja suunnitella kriteerit, joiden mukaan se tapahtuu. Configuration Managerilla luotiin kokoelma F-Secure-laitteille, jotka voitiin lukea pois kriteerejä tehtäessä. Tämä oli tärkeää, koska eri tietoturvaohjelmistot samassa tietokoneessa voivat aiheuttaa internetyhteyksien jumittumisen tai vastaavaa häiriötoimintaa. Ikävä kyllä kriteerejä tehtäessä oli tapahtunut virhe ja FEP 2010 asentui myös laitteisiin, joissa oli F_Secure asennettuna. Tämä sekoitti kyseisten laitteiden internet-yhteyden pariksi päiväksi kunnes virhe saatiin korjattua. Onneksi FEP 2010 on mahdollista poistaa yhtä helposti Configuration Managerin mainostustyökaluilla, kuin se on asentaa.

Projektin lopuksi FEP 2010 todettiin toimivaksi tietoturvaratkaisuksi, joka olisi tarkoitus ottaa laajempaan käyttöön myöhemmin. Tämä on siksi, että muun muassa laitoksen SCCM-palvelin päivitetään uuteen versioon, jolloin FEP 2010 pitäisi ottaa käyttöön uudelleen. Nykyinen F-Securen tietoturvaratkaisu toimii moitteettomasti, joten ongelmaa ei ole. Uusi SCCM-palvelin tulee käyttämään System Center Configuration Manager 2012 -versiota, jolle asennettaisiin Forefront Endpoint Protection 2012. FEP 2012 -laitteistovaatimukset ja asennus toimenpiteet säilyvät lähes samoina nykyiseen versioon verrattuna, joten tässä insinöörityössä käydyt asiat pitäisi olla mahdollista soveltaa myös FEP 2012:n käyttöönotolle.

Lähteet

1 9 Dirty Tricks: Social Engineer's Favorite Pick-Up Lines. Verkkodokumentti. <http://www.csoonline.com/article/480589/9-dirty-tricks-social-engineers-favorite-pick-up-lines?page=1>. 16.2.2009.

2 Consumer Advice: How to Avoid Phising Scams. Verkkodokumentti. <http://www.antiphishing.org/consumer_recs.html>.

3 Wikipedia. Brute-force.Verkkodokumentti. <http://en.wikipedia.org/wiki/Brute-force_attack>. 10.11.2011.

4 Microsoft Endpoint Protection 2010. Overview. Verkkodokumentti. <http://www.microsoft.com/en-us/server-cloud/forefront/endpoint-protection-overview.aspx>.

5 Microsoft System Center Configuration Manager. Overview. Verkkodokumentti. <http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-overview.aspx>.

6 SQL Server 2008 R2 Reporting Services Datasheet. PDF-asiakirja. <http://download.microsoft.com/download/C/F/0/CF03D712-1F02-4096-B631-88114C036233/SQLServer2008_R2_ReportingServices_Datasheet.pdf>.

7 Microsoft Forefront TechCenter. System Requirements. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/ff823876.aspx>.

8 Microsoft Forefront TechCenter. About Basic with Remote Reporting Database Setup. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/ff823821.aspx>.

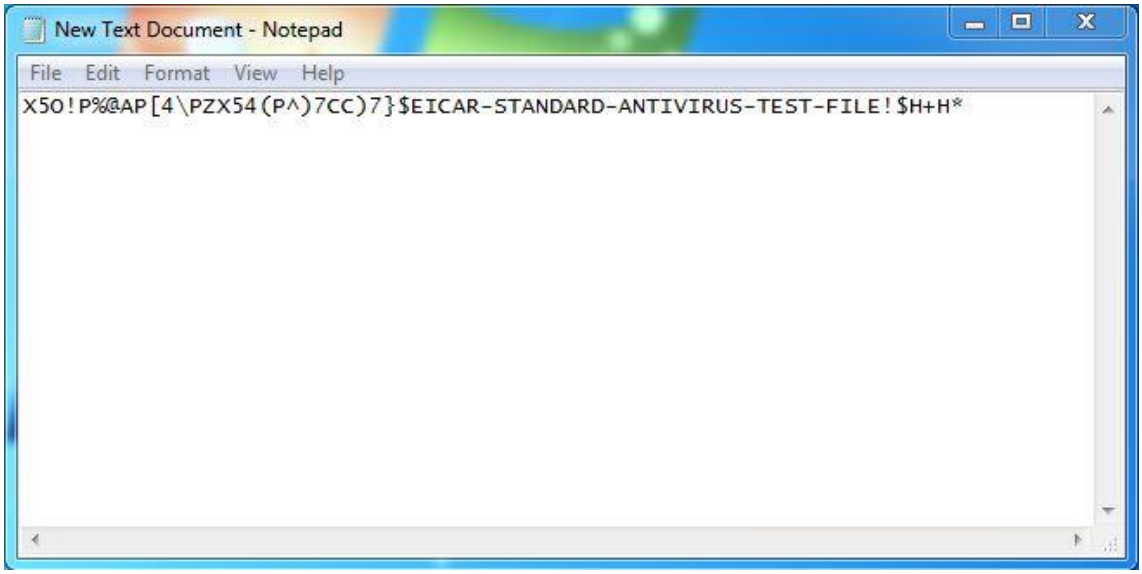
9 Microsoft Forefront TechCenter. What are recommended actions? Verkkodokumentti. <http://technet.microsoft.com/en-us/library/ff823813.aspx>.

10 Indiana University Knowledge Base. What is UNC? Verkkodokumentti. <http://kb.iu.edu/data/aibg.html>. 23.2.2011.

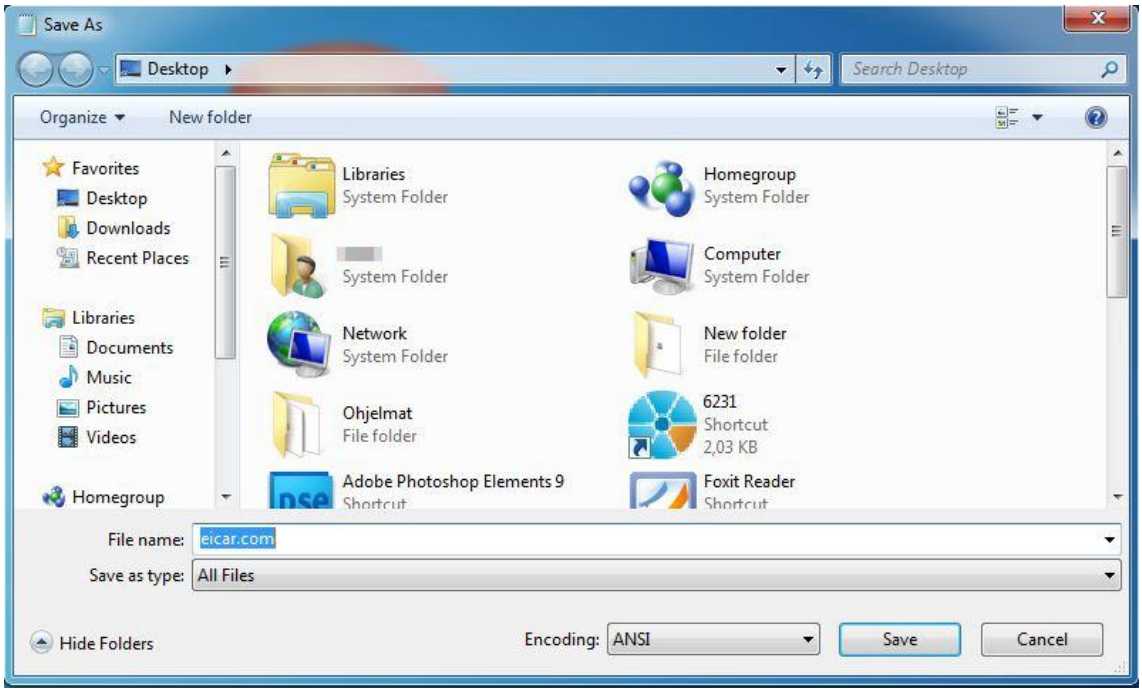
11 Windows Server. Windows Server Update Services. Verkkodokumentti. <http://technet.microsoft.com/en-us/windowsserver/bb332157>.

12 Windows Dev Center – Desktop. Querying with WQL. Verkkodokumentti. <http://msdn.microsoft.com/en-us/library/windows/desktop/aa392902(v=vs.85).aspx>.

Eicar testivirus



Kuva 1. Tehdään uusi tekstitiedosto notepadilla ja kirjoitetaan seuraava eicar-testiviruksen skriptikoodi sisällöksi.



Kuva 2. Tiedosto tallennetaan eicar.com nimellä, jolloin virustorjunnan pitäisi huomata virus tallentaessa.